Backgrounder No. 1 - The CSIS Mandate

Revised February 2005

The Canadian Security Intelligence Service (CSIS) was created by an Act of Parliament in 1984, following the McDonald Commission of Inquiry in the late 1970s and the Mackenzie Commission of the 1960s. The CSIS Act established a clear mandate for the Service and, for the first time, legislated a framework of democratic control and accountability for a civilian Canadian security intelligence service.

In meeting its mandated commitments, CSIS provides advance warning to government departments and agencies about activities which may reasonably be suspected of constituting threats to the country's security. Other departments and agencies, not CSIS, are responsible for taking direct action to counter security threats.

CSIS does not have law enforcement powers, therefore, all law enforcement functions are the responsibility of police authorities. The splitting of functions, combined with comprehensive legislated review mechanisms, ensures that CSIS remains under the close control of the federal government.

In its early years, much of the Service's energy and resources were devoted to countering the spying activities of foreign governments. Time has passed however, and as the world has changed, so has CSIS.

In response to the rise of terrorism worldwide and with the demise of the Cold War, CSIS has made public safety its first priority. This is reflected in the high proportion of resources devoted to counter-terrorism. CSIS has also assigned more of its counter-intelligence resources to investigate the activities of foreign governments that decide to conduct economic espionage in Canada so as to gain an economic advantage or try to acquire technology in Canada that could be used for developing weapons of mass destruction.

Along with these operational changes, CSIS has matured into an organization with a flexible, dynamic structure and, most importantly, an ingrained understanding of its responsibilities and obligations to Canadians. The Service's main purpose is to investigate and report on threats to the security of Canada.

This occurs within a framework of accountability to government, as well as respect for the law and the protection of human rights. Nowadays, it also means being more open and transparent to the people it serves. There are some limits on what the Service can discuss; that is the nature of its work, but CSIS is anything but a secret organization.

The Canadian way of life is founded upon a recognition of the rights and freedoms of the individual. CSIS carries out its role of protecting that way of life with respect for those values. To ensure this balanced approach, the CSIS Act strictly limits the type of activity that may be investigated, the ways that information can be collected and who may view the information. The Act provides many controls to ensure adherence to these conditions.

Information may be gathered, primarily under the authority of section 12 of the CSIS Act, only about those individuals or organizations suspected of engaging in one of the following types of activity that threaten the security of Canada, as cited in section 2:

1. Espionage and Sabotage

Espionage: Activities conducted for the purpose of acquiring by unlawful or unauthorized means information or assets relating to sensitive political, economic, scientific or military matters, or for the purpose of their unauthorized communication to a foreign state or foreign political organization.

Sabotage: Activities conducted for the purpose of endangering the safety, security or defence of vital public or private property, such as installations, structures, equipment or systems.

2. Foreign-influenced Activities

Foreign-influenced activities: Activities detrimental to the interests of Canada, and which are directed, controlled, financed or otherwise significantly affected by a foreign state or organization, their agents or others working on their behalf.

For example: Foreign governments or groups which interfere with or direct the affairs of ethnic communities within Canada by pressuring members of those communities. Threats may also be made against relatives living abroad.

3. Political Violence and Terrorism

Threat or acts of serious violence may constitute attempts at compelling the Canadian government to respond in a certain way. Acts of serious violence cause grave bodily harm or death to persons, or serious damage to or the destruction of public or private property, and are contrary to Canadian law or would be if committed in Canada. Hostage-taking, bomb threats and assassination attempts are examples of acts of serious violence that endanger the lives of Canadians. Such actions have been used in an attempt to force particular political responses and change in this country.

Exponents and supporters of political, religious or ideological violence may try to use Canada as a haven or a base from which to plan or facilitate violence in other countries.

Such actions compromise the safety of people living in Canada and the capacity of the Canadian government to conduct its domestic and external affairs.

4. Subversion

Subversion: Activities intended to undermine or overthrow Canada's constitutionally established system of government by violence. Subversive activities seek to interfere with or ultimately destroy the electoral, legislative, executive, administrative or judicial processes or institutions of Canada.

Lawful Protest and Advocacy

The CSIS Act prohibits the Service from investigating acts of advocacy, protest or dissent that are conducted lawfully. CSIS may investigate these types of actions only if they are carried out in conjunction with one of the four previously identified types of activity. CSIS is especially sensitive in distinguishing lawful protest and advocacy from potentially subversive actions. Even when an

investigation is warranted, it is carried out with careful regard for the civil rights of those whose actions are being investigated.

Security Screening

As well as investigating the four types of threats to Canadian security, CSIS provides security assessments, on request, to all federal departments and agencies with the exception of the Royal Canadian Mounted Police (RCMP), which conducts its own. These assessments are made with respect to applicants for positions in the Public Service of Canada requiring a security clearance, and for immigration and citizenship applicants

Security Assessments

The purpose of security assessments is to appraise the loyalty to Canada and reliability, as it relates thereto, of prospective government employees. The intent of the exercise is to determine whether persons being considered for security clearances are susceptible to blackmail or likely to become involved in activities detrimental to national security, as defined in section 2 of the CSIS Act. The assessments serve as a basis for recommending that the deputy head of the department or agency concerned grant or deny a security clearance to the individual in question. Security assessments are conducted under the authority of sections 13 and 15 of the CSIS Act.

The designated manager in the department or agency determines the security clearance level required for the position to be filled, in accordance with the standards set out in the Government Security Policy. CSIS then conducts the appropriate checks. The duration and depth of the investigation increase with the clearance level.

Immigration and Citizenship

Sections 14 and 15 of the CSIS Act authorize the Service to provide security assessments for the review of citizenship and immigration applications to the Department of Citizenship and Immigration.

The assessments provided by the Service for this purpose pertain to the provisions of section 2 of the CSIS Act that deal with threats to the security of Canada. The Department of Citizenship and Immigration uses these assessments to review immigration applications in accordance with the inadmissibility criteria set out in the Immigration and Refugee Protection Act. On 1 February 1993, this Act was amended to include, the terms "terrorism" and "members of an organization". This measure has increased the pertinence of CSIS assessments. Moreover, the inadmissible classes now include, in section 19(1)(f), persons who have engaged, or are members of an organization that has engaged, in acts of terrorism or espionage.

The same practice is followed for citizenship applications. They too are examined on the basis of the definition of threats to the security of Canada set out in section 2 of the CSIS Act, and security assessments are provided under section 19 of the Citizenship Act.

Questions & Answers

How and when was CSIS created?

CSIS was created by the passage of an Act of Parliament (Bill C-9) on June 21, 1984. The Service began its formal existence on July 16, 1984.

What does CSIS do?

CSIS has a mandate to collect, analyze and retain information or intelligence on activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and in relation thereto, report to and advise the Government of Canada. CSIS also provides security assessments, on request, to all federal departments and agencies, with the exception of the RCMP.

What organization collected security intelligence before CSIS was created?

Prior to June 21, 1984, security intelligence was collected by the Security Service of the RCMP. CSIS was created because the Government of Canada, after intensive review and study, came to the conclusion

that security intelligence investigations would be more appropriately handled by a civilian agency. CSIS has no police powers. However, CSIS works with various police forces on those investigations that have both national security and criminal implications. Although CSIS can offer assistance to the police, it has no mandate to conduct criminal investigations.

What constitutes a threat to the security of Canada?

The complete threat definitions can be found in section 2 (a,b,c,d) of the CSIS Act. Simply put, terrorism (the planning or use of politically motivated serious violence) and espionage (undeclared foreign intelligence activity in Canada and detrimental to the interests of Canada) are the two major threats which CSIS investigates. Terrorism and espionage can have criminal implications. In such cases, the RCMP investigates and can lay the appropriate criminal charges.

What is "security intelligence" and does the government really need it given that technology allows news broadcasters to deliver information from around the world in a matter of minutes?

Security intelligence is information formulated to assist government decision-makers in developing policy. Regardless of the source of intelligence, it provides value in addition to what can be found in other government reports or in news stories. Intelligence conveys the story behind the story.

How does CSIS obtain this "value-added" component?

The "value-added" comes from analysis and a wide variety of investigative techniques, including the use of covert and intrusive methods such as electronic surveillance and the recruitment and tasking of human sources.

Can these techniques be arbitrarily deployed?

No. All intrusive methods of investigation used by CSIS are subject to several levels of approval before they are deployed. The most intrusive methods-such as electronic surveillance, mail opening and covert searches-require a warrant issued by a judge of the Federal Court of Canada. In addition, the Security

Intelligence Review Committee and the Inspector General closely review CSIS operations to ensure they are lawful and comply with the Service's policies and procedures.

What does CSIS do with the security intelligence it collects?

CSIS reports to and advises the Government of Canada. CSIS intelligence is shared with a number of other federal government agencies and departments, including the RCMP and the departments of Foreign Affairs and International Trade, Citizenship and Immigration, and of National Defence. As well, CSIS has arrangements to exchange security-related information with other countries. The vast majority of these arrangements deal with visa vetting. A small number deal with exchanges of information collected by CSIS in its investigation of threats to national security.

What is the difference between a security intelligence service and a foreign intelligence service?

A security intelligence service is restricted to investigating threats to its country's national security. A foreign intelligence service, on the other hand, conducts offensive operations for its government in foreign countries. The methods and objectives of foreign intelligence services differ from country to country.

Does CSIS have any foreign presence at all?

CSIS has liaison offices in some countries. Liaison officers are involved in the exchange of security intelligence information which concerns threats to the security of Canada.

Does CSIS investigate industrial espionage?

CSIS does not investigate company-to-company industrial espionage. CSIS does, however, investigate the activities of foreign governments that engage in economic espionage as a means of gaining an economic advantage for themselves. Economic espionage can be defined as the use of, or facilitation of, illegal, clandestine, coercive or deceptive means by a foreign government or its surrogates to acquire economic intelligence.

What is the impact of foreign government economic espionage activity on businesses in Canada?

Foreign government economic espionage activity exposes Canadian companies to unfair disadvantage, jeopardizing Canadian jobs, Canada's competitiveness and research & development investment.

Does CSIS conduct investigations on university campuses?

CSIS is very sensitive to the special role that academic institutions play in a free and democratic society and the need to preserve the free flow of ideas, therefore, investigations involving university campuses require the approval of senior officials in the Service. Furthermore, human sources and intrusive investigative techniques may only be used with the approval of the Minister for Public Safety and Emergency Preparedness.

Can you name individuals or groups currently under CSIS investigation?

The CSIS Act prevents the Service from confirming or denying the existence of specific operations. To disclose such information would impede the Service's investigative capabilities which, in turn, would be injurious to national security. CSIS, however, can assure the public that it is doing everything within its mandate to ensure that Canadians are safeguarded from terrorism and foreign espionage.

Given that the Cold War is over, are there still threats with which Canadians should be concerned?

Yes. Details regarding the Service's view of the security intelligence environment can be found in its annual Public Reports.

ARCHIVED: Backgrounder No. 2 - Accountability and Review

Backgrounder No. 2 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

November 2004

Intrusive methods are sometimes required to fulfil the mandate of the Canadian Security Intelligence Service (CSIS). As such, ensuring that there is an effective system to provide direction, management and accountability is of primary importance. The system that was laid down in the CSIS Act is composed of a series of interlocking parts resulting in CSIS being one of the most open and accountable security intelligence organizations in the world.

1. Ministerial Responsibility

The Minister of Public Safety and Emergency Preparedness (PSEP) is responsible to Parliament for CSIS as a whole and for its general direction. The Minister also issues policy guidelines concerning basic operational procedures and is informed of security operations and problems, should they arise, by the Deputy Minister, the Director of CSIS, and the Inspector General.

2. Deputy Solicitor General

The Deputy Minister has a statutory duty to consult on general operational policies and to provide advice to the Minister on the need for general direction to CSIS, as well as how the Service implements this direction. Through involvement in the warrant application process, the Deputy Minister is kept aware in advance of related operational activities.

3. The Director

The Director of CSIS is responsible to the Minister for the control and management of the Service. The Director must consult with the Deputy Minister on the operational policy of CSIS, on applications for warrants, and on any other matter for which the Minister indicates such consultation is needed. The Director also submits periodic reports on CSIS activities to the Minister. Finally, the Director chairs a number of internal committees which further enhance the management and accountability of CSIS. Two of these committees have direct responsibility for, and authority over, the Service's use of investigative techniques.

4. Inspector General

The Inspector General, created by Parliament in the CSIS Act, reports through the Deputy Minister to the Minister. The Inspector General is responsible for monitoring the Service's compliance with its operational policies, reviewing the operational activities of CSIS and submitting a certificate setting out the degree of satisfaction with the Director's annual operational report. The certificate and the report are forwarded by the Minister to the Security Intelligence Review Committee (SIRC). At the request of the Minister or SIRC, the Inspector General may conduct research and enquiries.

5. Security Intelligence Review Committee (SIRC)

The Security Intelligence Review Committee (SIRC) is an independent review agency which guards against any infringement upon human rights and freedoms by CSIS. SIRC was created by Parliament in the CSIS Act.

SIRC is composed of between three and five Privy Councillors who are not members of the House of Commons or the Senate. SIRC members are appointed by the Governor in Council. Prior to making these appointments, the Prime Minister consults the Leader of the Opposition and the leader of any party that has at least 12 members in the House of Commons.

The Committee's responsibilities are extensive. First, SIRC reviews the Service's performance of duties and functions, especially with reference to the Director's reports to the Minister, the Inspector General's certificates, and the directions of the Minister to the Director.

Second, SIRC investigates the complaint of any person with respect to any act performed by the Service. The Committee also investigates complaints from those individuals denied security clearances in the cases of public service employment, or in the supply of goods or services to the Government of Canada. In addition, SIRC receives reports concerning immigration applications and may receive reports concerning citizenship applications which have been rejected on security or criminal grounds.

Commensurate with these responsibilities, SIRC has been granted special powers. The Committee has access to all information under the Service's control, with the exception of Cabinet confidences, as does the Inspector General. SIRC has the authority to direct the Inspector General to examine specific activities. It may also conduct such investigations utilizing its own staff.

The analyses by SIRC of the Service's performance are provided to the Minister on an ongoing basis. In addition, the Committee is required to produce an annual report which is presented to the Minister for tabling in Parliament.

6. Judicial Control

Prior to the formation of CSIS, the use of intrusive investigative techniques was authorized by the then Solicitor General. Today, only the Federal Court of Canada can authorize such a warrant. The warrant itself is the end product of a long and intensive decision-making process. The warrant's affidavit, which establishes the justification for an intrusive investigative technique, must first be reviewed by CSIS managers, and subsequently by a senior committee within the Service chaired by the Director. This committee includes representatives from the Department of Justice and PSEP. If the decision is to proceed with the warrant application, the affidavit is then submitted to the Minister of PSEP, who must

approve it personally. Only after receiving the Minister's approval is the affidavit submitted to a judge of the Federal Court for a decision.

7. Parliament

A Special Committee on the Review of the CSIS Act and the Security Offences Act was established by an order of the House of Commons dated June 27, 1989. This order, based on the stated requirement in section 56 of the CSIS Act, required the Committee to undertake a comprehensive review of the provisions and operation of both the CSIS Act and the Security Offences Act and to report its findings to the House of Commons. These findings are the subject of a report entitled In Flux But Not In Crisis.

The five-year review committee was later reconstituted as the Sub-Committee on National Security of the Standing Committee on Justice and the Solicitor General. Its work plan has included reviewing the functions of CSIS. In addition, the Committee has considered reports made by SIRC, the annual statement of the Minister with respect to National Security, and the Public Report from the Director of CSIS.

8. The CSIS Public Report

In 1991, the Government of Canada responded to the Five-Year Parliamentary Review Committee's report on the CSIS Act and the Security Offences Act with On Course. In On Course, the Government of Canada made a commitment to provide Parliament with more information on the national security system. This stems from the recognition that effective legislative control over CSIS must be accompanied by increased public knowledge about its role. The Minister of PSEP and CSIS meet this commitment by providing Parliament and the public with the Minister's Annual Statement on National Security and the CSIS Public Report and Program Outlook.

The Minister is responsible for three main elements of the national security system. These elements are security intelligence; security enforcement; and protective security. The Minister's Annual Statement on National Security is an overview of these three elements. Taken together, the Statement and the CSIS Public Report are intended to provide Canadians with an assessment of the current security intelligence environment and the government's efforts to ensure national security

The CSIS Public Report discusses Canada's security environment and CSIS' national security role. The purpose of the Report is to increase public knowledge about CSIS' mandate and improve understanding of how the national security of Canada is safeguarded by the Service, with due respect for individual rights and freedoms. The report also addresses many of the popular myths surrounding security intelligence work.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

ARCHIVED: Backgrounder No. 3 - CSIS and the Security Intelligence Cycle

Backgrounder No. 3 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

Revised February 2004

The primary mandate of CSIS is to collect and analyze information and subsequently to provide reports, in the form of security intelligence, to the government. CSIS produces intelligence in order to provide advance warning to government departments and agencies about activities which may reasonably be suspected of constituting threats to Canada's security. One of the primary values of intelligence-gathering is the timely delivery of perishable information to policy-makers in government. The five phases of the process that produces these results is known as the security intelligence cycle and they are described in this backgrounder.

1. Government Direction

CSIS responds to direction from the federal government. This is the central characteristic of the relationship envisioned in the CSIS Act. The Act ensures that the Minister of Public Safety and Emergency Preparedness has the responsibility to provide direction to the Director of CSIS on matters

concerning the policies, operations and management of CSIS. Policy guidelines for Service activities are established through these directives. Direction of this nature covers many areas of Service activity, including guidance in the use of investigative methods and techniques. It also ensures that the Minister is a key decision-maker within the Service's legal and policy framework.

Regular direction from government on intelligence priorities is one characteristic that distinguishes the Service from a police organization. Police agencies conduct criminal investigations based upon the law. Security intelligence work is rooted in government priorities formulated within the context of the legislative framework of the CSIS Act.

Intelligence priorities are re-evaluated each year in light of an annual assessment by the Service. This assessment is based on the Service's review of the constantly changing security environment. CSIS has established an ongoing environmental scanning capability in order to integrate government requirements more directly into the intelligence cycle. Based on consultations with other government departments and agencies, an assessment is then provided to the government. Following ministerial consideration of the assessment, the Minister then provides direction to the Service.

The Service has established a Government Liaison Unit which is responsible for maintaining regular contact with departments in order to obtain their security intelligence requirements. This enables the Service to tailor distribution of its information to a department's specific requirements.

2. Planning

Planning encompasses the entire intelligence process, which begins with the threat assessment phase and culminates with the delivery of the final intelligence products. Plans are geared to meet the government's security intelligence requirements. In response to client needs and ministerial direction, CSIS determines a co-ordinated strategic approach. In this way, resources are allocated for investigations on the basis of government-approved criteria.

In planning an investigation, care is taken to ensure an appropriate balance between the degree of intrusiveness of an investigation and concern for the rights and freedoms of those being investigated. Low-level investigations, consisting primarily of the collection of open-source information, may be approved by operational supervisors. Investigations which may call for the use of more intrusive techniques are subject to a rigorous process of challenge and controls, including a review by senior

management committees chaired by the CSIS Director, with representation from the departments of Justice and Public Safety and Emergency Preparedness.

All investigative activities must abide by ministerial direction. Section 21 of the CSIS Act requires that judicial authorization in the form of a Federal Court warrant must be obtained before certain intrusive techniques are used. A Federal Court judge must be satisfied, after examining a CSIS draft warrant and accompanying affidavit, that there are reasonable grounds to justify issuing such a warrant.

3. Collection

Collection is the preliminary phase of the Service's advisory role to government. Information from members of the public, foreign governments and technical interception of communications are combined with information from open sources including newspapers, periodicals, academic journals, foreign and domestic broadcasts, official documents and other published material.

The Service uses a variety of collection methods to monitor individuals or groups whose activities are suspected of constituting a threat to national security. Through such monitoring, the Service can identify individuals with suspected connections to terrorism and persons operating in Canada on behalf of hostile intelligence services. In addition to monitoring potential espionage and sabotage efforts, the Service is mandated to inform the government of foreign-influenced activities within or relating to Canada that are detrimental to the interests of this country, are clandestine or deceptive, or involve a threat to any person.

In the competitive global economy of the 1990s, acquiring scientific and technological information from other countries has become increasingly important for many nations. Sometimes, this is done by covert or unlawful means. As a result, CSIS has intensified its activities to detect economic espionage against Canadian scientific and technological interests by foreign governments and/or their surrogates.

CSIS maintains full-time security liaison officers at a number of Canadian diplomatic missions abroad. Their task is to work with selected foreign police and security intelligence agencies. They also collect and analyze openly available information on global trends which may have Canadian security implications, and, finally, they conduct security screening assessments of prospective immigrants.

4. Analysis

Policy makers rely on security intelligence prepared by Service analysts following the information collection stage. Analysts in all operational programs use their knowledge of regional, national and global trends to assess the quality of all types of information gathered, and organize it into useful security intelligence.

Information collected by investigators is initially assessed at a regional office prior to its transmission to CSIS Headquarters in Ottawa, where a second-phase analysis is undertaken from a national perspective. This investigative reporting is then combined with information gathered from consultations with government agencies, other intelligence agencies and open sources. Further analysis of the information is carried out within an intelligence analysis program dedicated to the preparation of CSIS intelligence reports.

As part of the broader Canadian security intelligence analysis and assessment effort, CSIS also participates in the Intelligence Assessment Committee of the Privy Council Office, which reports to the Interdepartmental Committee on Security and Intelligence. This committee is chaired by the Clerk of the Privy Council and consists of deputy-minister-level officials of departments and agencies active in the security and intelligence field, including CSIS.

5. Dissemination

The CSIS Act designates the Government of Canada as the main recipient of CSIS intelligence. Under section 19 of the CSIS Act, the Service distributes a variety of reports, including threat assessments, to various departments of the federal government and law enforcement authorities.

The RCMP depends on threat assessments to determine the level of security required to protect foreign diplomatic missions and Canadian VIPs. The Department of Foreign Affairs and International Trade uses these threat assessments to determine the proper level of protection required for Canadian missions and personnel overseas. Transport Canada uses the assessments when considering security concerns for the travelling public.

Under the Government Security Policy, CSIS also undertakes threat and risk assessments for departments and their operating programs at their request.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

ARCHIVED: Backgrounder No. 4 - Human Resources

Backgrounder No. 4 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

Revised February 2004

History

The Mackenzie Commission of 1969 and the McDonald Commission of 1977 recommended that, in order to balance the need for accurate and effective security intelligence with the need to respect democratic rights and freedoms, Canada's security intelligence functions should be separated from the RCMP and that a civilian service should be formed.

In August 1981, the federal government announced that the Canadian Security Intelligence Service would be created.

The establishment of CSIS by an Act of Parliament in 1984 recognized the differences between security intelligence activities and law enforcement work, bringing an end to the 120-year-old interlocking of Canada's security intelligence service with the RCMP.

The CSIS Act was given Royal Assent in June 1984, and CSIS began its formal existence on July 16, 1984.

At that time, the new Service had a staff of 1,968. CSIS staff occupied eight separate buildings throughout Ottawa, working in operational units for counter-intelligence, counter-terrorism, counter-subversion and security screening during the early months of the new organization's existence. The distribution of resources for counter-intelligence was four times greater than for counter-terrorism in those early days.

In 1987, the Solicitor General tabled in the House of Commons the third Annual Report of the Security Intelligence Review Committee (SIRC). In its report, SIRC raised a number of concerns about CSIS, prompting the Solicitor General to announce the formation of an independent advisory team headed by Gordon Osbaldeston, former Clerk of the Privy Council, to study several specific issues raised by SIRC and present a plan of action to the Solicitor General.

One of the issues studied by the advisory team was whether CSIS policies on recruitment, training & development and personnel management had provided the Service with the proper mix of skills, education and experience to meet the intelligence requirements of the government.

Regarding the adequacy of CSIS resources, the Osbaldeston Report concluded that, with the proclamation of the CSIS Act: " ... a number of new requirements were also created, many of which had to be provided from scratch. Among them were a complete management structure, an administrative system to provide the support previously drawn from the RCMP, accommodation separate from the RCMP, new communications and computer systems and a methodology for dealing with a complicated system of external review. All of this was to be provided, as a former member of CSIS management put it, ?on a shoestring'. The turmoil generated in simply getting CSIS established is a factor often overlooked by the critics," the Report said.

Among many other things, the Report recommended a complete review of all CSIS capital and operating resource requirements to determine a basis " ... from which to set reasonable and adequate resource levels for the Service." The government responded by providing additional funding over four years for personnel and operating requirements. The report also called for an "immediate" solution to the problem created by having a staff that was by 1987 at a level of 2,153 operating in separate buildings throughout Ottawa. The government responded with a commitment to construct the new headquarters building at a total cost of $151 million. The new building houses all CSIS headquarters personnel under one roof. Construction of the facility was completed in 1995 within the approved budget.

Looking back on implementation of the government's decision to establish CSIS, the Osbaldeston Report noted the Security Intelligence Review Committee's concern that the counter-subversion program "... casts its net too widely". Osbaldeston recommended that the counter-subversion branch be eliminated, and that its duties and functions be reassigned. The Service responded by eliminating the counter-subversion program as a separate organizational entity.

With the number of terrorist incidents accelerating dramatically in the eighties, worldwide patterns and the scope of terrorist incidents became more and more apparent. One of the consequences was that terrorism became increasingly defined as an intelligence problem as well as a police matter. In Canada, counter-terrorist activity increased following the 1982 assassination of a Turkish military attaché en route to work in Ottawa, and the 1985 takeover of the Turkish Embassy, in which a security guard was killed. Air India Flight 182 was downed off the coast of Ireland in 1985, resulting in the deaths of all 329 people on board, most of whom were Canadians.

Partly as a direct response to these developments, counter-terrorism resources, including personnel, were increased during 1986 and 1987. As a consequence of the dramatic changes to the security environment in the past twenty years, there has been a continuing adjustment of operational resources to match the changes in the security environment. Particularly the September 11, 2001 terrorist attacks on the World Trade Center and the ensuing global response to terrorism prompted further adjustments to Service resources. In 2002, a counter-proliferation responsibility centre was created within CSIS to answer the growing threat to international peace and security from weapons of mass destruction.

Resource Profile

Since its inception, the Service has experienced significant shifts in its human resource levels. The government's restraint program and Program Review exercises resulted in a decreased workforce between 1992 and 1998, where its complement was reduced by 28 percent or 760 positions. The impact of Program Reviews and other reductions brought the Service's human resource level down to 2000 FTEs in 1997/1998.

The Service was able to adjust to staff reductions through normal attrition and by focusing on reducing administrative overhead to the extent possible and relying upon technological innovations to realize efficiencies.

In 1998, the Service assumed responsibility for the security screening of employees of the Department of National Defence (DND), which augmented the Service's base budget through a transfer of resources from DND. Since then, there have been ongoing increases to the FTE level due to increased immigration security screening requirements. Resource levels also increased in fiscal year 1999/2000, due to Year 2000 requirements.

Finally, following the terrorist attacks on the World Trade Center on September 11, 2001, the government approved additional funding in an effort to bolster its counter-terrorism capabilities, resulting in the Service's human resource level reaching 2380 FTEs by fiscal year 2006/2007.

The Service is dealing with staff increases through a targeted recruitment strategy. Special emphasis will continue to be placed on maintaining the operational integrity of the Service, and essential positions must continue to be staffed by people with the qualifications and specialized skills related to security intelligence. Therefore, the Service will continue to recruit high-calibre university graduates to become intelligence officers.

A Representative Workforce

Because CSIS is a national organization, it maintains a presence throughout the country. Nearly half of its workforce is based in six regions extending from the Maritimes to British Columbia. Most regions have a head office and district offices. The remaining CSIS employees are located at Headquarters, in Ottawa. The Service tries to ensure that the various ethnic groups that constitute the Canadian mosaic are equitably represented in its workforce.

As a federal institution, CSIS ensures that the objectives of the Official Languages Act are met within the Service. CSIS is committed to ensuring: that communications with the public take place in both official languages as required by the Act; that work environments promote the use of either official language by the employees in the regions described in the Act; and that its workforce reflect the presence of the two official language communities in Canada, while endeavouring to provide equal opportunities for employment and advancement within the Service to both English- and French-speaking Canadians.

CSIS also ensures that programs and strategies are developed to assist managers in the recruitment, development and retention of persons who are members of the four employment equity designated groups: women, visible minorities, persons with disabilities and aboriginal peoples.

Training and Development

CSIS is committed to fostering a work environment in which its employees are constantly learning and developing professionally. To this end, employees can participate in both internal or external courses and seminars that allow them to develop new skills, acquire knowledge, or gain new perspectives in areas that will help them perform their duties.

The Service's internal training and development program is comprehensive, covering a full range of training and seminars related to management, professional development, informatics, as well as operational matters. External courses are used to enhance employees' skills on non-CSIS specific topics.

Recruitment

The range of CSIS activities means that its employees must possess a variety of academic backgrounds and abilities. To operate effectively, the Service needs not only intelligence officers, but also scientists, engineers, technologists, translators/interpreters, technicians, information specialists (librarians, library technicians), financial and information technology specialists.

The intelligence officer category is the core professional group. They are responsible for the collection, analysis and production of intelligence. In order to be considered for employment in this category, the following qualifications are required:

- Canadian citizenship (applicable to all employees);

an undergraduate university degree;

the ability to physically relocate;

a valid driver's licence.

Meeting these requirements is only the starting point in applying to work at CSIS. The application process is rigorous, competitive and lengthy. Because of the sensitive nature of CSIS's work, all applicants must undergo security background investigations.

Canadian citizens interested in a career with CSIS are encouraged to apply on-line to the Canadian Security Intelligence Service's career Web site. When you submit your résumé to CSIS, your personal information will be protected under the federal Privacy Act.

Important note: Once you begin the process of filling in the on-line application form, you should not stop because the process could time-out. Therefore, applicants should make sure that the following information is readily available:

Previous employment information, including the names of previous employers and supervisors; dates, salaries, addresses and telephone numbers.

Information relating to education and training (degrees, diplomas, the name(s) of the institution(s) and dates attended).

A list of all foreign countries you have travelled to or lived in and when, excluding the USA, and whether the travel was for holiday, business, study or other reason.

Should you time-out before you have completed the application form, you will be required to re-register under a new username and password and start the process all over.

We thank all those who apply and advise that only those selected for further consideration will be contacted.

ARCHIVED: Backgrounder No. 5 - A Historical Perspective on CSIS

Backgrounder No. 5 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

Revised January 2001

The establishment of the civilian Canadian Security Intelligence Service and the disbanding of the Royal Canadian Mounted Police Security Service by an Act of Parliament in 1984 recognized the differences between security intelligence activities and law enforcement work. The 120-year old interlocking of Canada's security intelligence service with the federal police force was brought to a close.

The evolution towards the Canadian Security Intelligence Service began when Sir John A. Macdonald created the Western Frontier Constabulary in 1864. This was to be a "...detective and preventive police force, for the purpose of watching and patrolling the whole frontier from Toronto to Sarnia." The Constabulary operated along the Upper Canada borders and rail lines, reporting on activities related first to the American Civil War, then to Fenians whose goal was to overthrow English rule in Ireland. Eastern Canada was looked after by the Montreal Water Police, a federal agency like the Constabulary which was set up originally under William Ermatinger. He was later replaced by Joseph Coursol. Both forces reported to Macdonald.

In 1868 the government, responding to a perceived need, set up a 12-member Dominion Police force in charge of guarding public buildings and carrying out the previous responsibilities of the Western Frontier Constabulary. This force, under Gilbert McMicken and Coursol, assigned people to a security intelligence

function when it was necessary, returning them to regular duties afterwards. By the beginning of the First World War, there were 140 members.

The Dominion Police, with Canada's developing security intelligence function, was amalgamated with the 2,500 members of the Royal North West Mounted Police in 1920 to form the Royal Canadian Mounted Police. Between the wars, the security intelligence function remained small and inconspicuous. At the headquarters in 1939, it employed only three members and two stenographers, with field units in the larger cities investigating threats such as the fascist movement. The espionage activity related to the Second World War, and the subsequent defection of Soviet cypher clerk Igor Gouzenko in September 1945, removed any thoughts the government might have had about reducing the security intelligence function to pre-war levels.

Gouzenko's revelations of a number of elaborate Soviet espionage networks operating in Canada ushered in the modern era of Canadian security intelligence. Previously, the "communist menace" had been viewed by authorities in terms of its threat to the labour movement. Gouzenko's information showed that the Soviets of the day were interested in more than cultivating disaffected workers: they were intent on acquiring military, scientific and technological information by whatever means available to them. Such knowledge had become the key to advancement, and the Soviets intended to progress. Thus, as the post-war period gave way to the Cold War, Canadian security intelligence operations grew in response to this new threat.

Espionage, however, soon became only one aspect of the complex world facing those involved in Canadian intelligence work. The 1960s provided challenges of an entirely different and unprecedented order. In Quebec, members of the Front de libération du Québec (FLQ) emerged and used assassination, kidnapping, bombing and other acts of terrorism in attempting to achieve their political goal. Other events, such as the debate over the deployment of nuclear weapons on Canadian soil, the escalating involvement of the United States in Vietnam, and the evolution of a vigorous peace movement carried a potential for politically motivated violence, foreign-influenced activities and subversion. It was necessary to identify potential threats, but in order to fully maintain the democratic way of life of Canadians, it was also necessary to scrupulously protect the right to exercise legitimate political dissent.

These tasks were made all the more complex by the conflicting combination of priorities and responsibilities of security intelligence investigations as compared to police work. Two different Commissions chaired by Justice Mackenzie in 1969 and Justice McDonald in 1977 recommended that the security intelligence functions be separated from the RCMP and that a civilian service be formed to carry out those functions. Both commissions recognized that the problem of balancing the need for

accurate and effective security intelligence with the need to respect democratic rights and freedoms could not be adequately resolved as long as security intelligence responsibilities remained part of the Federal police force.

In 1970, following the report of the MacKenzie Commission, John Starnes, a foreign service officer with the Department of External Affairs, became the first civilian Director General of the RCMP Security Service. Institutional links between the Security Service and the main body of the RCMP became more flexible, but problems, due to the different natures of security intelligence work and police work, remained. The establishment of a civilian security intelligence service came with the findings and recommendations of the McDonald Commission. In August 1981, the federal government announced that a security intelligence service, separate from the RCMP, would be created. A Security Intelligence Transition Group task force was formed to plan and oversee the establishment of the new organization.

The first legislation to establish the security intelligence service, Bill C-157 , "an Act to Establish the Canadian Security Intelligence Service (CSIS)", was introduced in Parliament in May 1983. In response to public concern about the legislation, a special committee of the Senate was established to examine the Bill. Chaired by Senator Michael Pitfield, it produced findings and recommendations in November 1983. Acting on suggestions in this report, the federal government tabled amended legislation, Bill C-9, in the House of Commons in January 1984. It was passed by both Houses of Parliament and given Royal Assent in June 1984. CSIS began its formal existence on July 16, 1984 with Ted Finn as Director. In addition to creating a civilian security intelligence service, the Act also created SIRC, to review the activities of CSIS.

In 1987, then Solicitor General of Canada James Kelleher directed former Clerk of the Privy Council Gordon Osbaldeston to review concerns raised by SIRC and present a plan of action. Osbaldeston's report recommended changes to the executive, proposed a new support infrastructure, and suggested elimination of the Counter-Subversion Branch. By 1988 the Service had a new Director, Reid Morden, and significant internal changes had been enacted, not the least of which had been the dismantling of the Counter-Subversion Branch as had been suggested.

The Act that created CSIS also sought to ensure that the Service would continue to develop as an effective and responsible organization. To this end, section 56 called for a comprehensive review of the provisions and operations of the CSIS Act to be undertaken after July 1989. As required, the five-year review called for in the CSIS Act was completed by a Special Committee of the House of Commons under Chairman Blaine Thacker. The Committee's report, In Flux But Not In Crisis, completed in September of 1990, declared that the Service and the Act were essentially on course, but provided recommendations for improvement nonetheless. The then Solicitor General of Canada, Pierre Cadieux, responded to these

recommendations in On Course, a study detailing the mandate and role of the Canadian Security Intelligence Service and the national security requirements and milieu in Canada.

A third review of the dynamics of national security was completed during 1992. In view of the changed geo-political circumstances brought about by the end of the Cold War, the Solicitor General asked then Director of CSIS, Ray Protti, to review the changing security intelligence environment to determine if the Service should restructure and what resources would be necessary to respond to the changing environment. The review concluded that the Service was essentially well-structured to respond to the changing security intelligence environment. Detailed results of this review were incorporated in the 1992 CSIS Public Report.

In 1994, Ward Elcock was appointed the new Director of CSIS.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

ARCHIVED: Backgrounder No. 6 - Economic Security

Backgrounder No. 6 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

Revised February 2004

"Our orientation in national security is influenced considerably by the global security environment. Just as our national security system has undergone adjustment and reorientation over the last ten years, so must we be ready to adapt and reorient in the coming years". The Hon. Herb Gray, former Solicitor General, Statement on National Security, April 11, 1994

The Hon. Herb Gray, former Solicitor General,

Statement on National Security, April 11, 1994

Introduction

The era when traditional global security relations overshadowed economic concerns and regional conflict has passed. Accelerating economic interdependence and international competition have emerged as major sources of tension and conflict among world powers. In this uncertain environment, developed countries eager to maintain their standards of living, and developing countries equally determined to improve their own, are under pressure to use whatever means they have to improve their productivity and ensure their economic security. One such means is economic espionage, which can be described as illegal, clandestine or coercive activity by a foreign government in order to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage.

Impact

Although some spectacular incidents have found their way into media reports, analysis of the overall impact of economic espionage is difficult because of industry's reluctance to discuss the issue in detail. In fact, the General Accounting Office - the investigative arm of the U.S. Congress - had to abandon its plan to study the extent and impact of foreign government spying on U.S. companies when it became clear firms had little desire to discuss the matter. Canadian explorations of the issue have met with similar responses. There are a number of reasons for this corporate reticence. In many cases, firms fear disclosure could harm their reputation, or undermine shareholder confidence.

Despite these obstacles to a formal calculation, business and government representatives generally agree that the cost of economic espionage activities to individual firms and the economies that host them is in the billions of dollars. In its new national survey, the American Society for Industrial Security (ASIS) estimated that intellectual property losses from foreign and domestic espionage may have exceeded $300 billion in 1997 alone. More than 1,100 documented incidents of economic espionage and 550 suspected incidents that could not be fully documented were reported last year by major U.S. companies. The 1997 survey revealed that high-tech companies were the most frequent targets of foreign spies, followed by manufacturing and service industries. Among the most sought-after information were research and development strategies, manufacturing and marketing plans, and customer lists. The Service estimates that the loss to Canadian firms may also be in the hundreds of millions of dollars.

The Canadian government has transformed its national requirements for security intelligence to reflect this modified threat environment. Currently, the government has identified economic security as one of its priorities. CSIS has responded to these changing dynamics and to their impact on Canadian defence,

foreign policy and economic interests. However, it is important to note that while economic security is of significant concern to CSIS, public safety is the Service's number one priority.

CSIS' Economic Espionage Mandate

Though there has been a decline in offensive intelligence operations directed against Canada by some members of the former Central and Eastern European services, a number of countries continue to carry out such activity . Moreover, increasing global economic competition is leading many governments to shift the focus of their intelligence collection away from the traditional areas of political and military matters to the illicit acquisition of economic and technological information. One of our primary objectives is to monitor the activities of known or suspected foreign intelligence officers in Canada, and to prevent foreign visitors, students and delegates suspected of intelligence activities from gaining access to the country.

CSIS' mandate relative to economic espionage is to investigate, when necessary, clandestine activities by foreign governments that are potentially detrimental to Canada's economic and commercial interests.

CSIS seeks to forewarn government when the otherwise level playing field of free market competition is deliberately tilted against Canadian industry.

CSIS does not investigate industrial espionage - the practice of one private sector company spying on another. If these activities are of a criminal nature, they may be investigated by law enforcement agencies. As well, civil remedies may be available.

The vast majority of economic intelligence gathered by businesses or governments is derived from open sources in a legal manner involving no clandestine, coercive or deceptive methods. The collection and dissemination of information in this manner, either through visiting scientists, students or businessmen, is rightly seen as a beneficial element of a free and open society. In a minority of cases, however, economic intelligence is obtained with questionable techniques and with less than desirable results.

1. The Global Environment

Economic Espionage in Canada

Canada is a world leader in many technology-intensive fields. Aerospace, biotechnology, chemical, communications, information technology, mining & metallurgy, nuclear, oil & gas and environmental technology are key industrial sectors in the Canadian economy. Canadian enterprises maintain and develop information and technology of economic significance, the protection of which is essential to their economic viability, and by extension, the economic well-being of Canada.

A number of Canadian companies operating in these sectors have been targeted by foreign governments to obtain economic or commercial advantages. The damage to Canadian interests takes the form of lost contracts, jobs and markets, and overall, a diminished competitive advantage. Information and technology that has been the target of economic espionage includes trade and pricing information, investment strategy, contract details, supplier lists, planning documents, research and development data, technical drawings and computer databases.

Examples

A Canadian company's technology was compromised when the company, hoping to secure a lucrative contract from a foreign government, allowed a national of that country to work on a sensitive, leading-edge technology project. The foreign government then proceeded to duplicate the technology using the information obtained through the direct access their representative agent had to this project.

In another instance, a foreign government is believed to have tasked its intelligence service to gather specific information. The intelligence service in turn contracted computer hackers to help meet the objective, in the course of which the hackers penetrated databases of two Canadian companies. These activities resulted in the compromise of numerous computer systems, passwords, personnel and research files of the two companies.

In another incident, a foreign scientist working in the biotechnology sector stole laboratory cultures and confidential manuals from a Canadian company which is believed, in the process, to have lost valuable R&D data, as well as potential earnings. It was later determined that the individual involved had also stolen similar materials from his previous employer based in another country.

There is no limit to ingenuity when it comes to the clandestine collection of significant economic information. The most frequently used collection method is the recruitment of someone who has access to the information (employees, contractors, consultants, students, etc.). However, other methods include break-ins, briefcase tampering, photocopying, garbage retrieval and communications interception. In the latter case, the means at the disposal of a foreign government to monitor telecommunications often exceed what is commercially available.

Economic Espionage Abroad

Businessmen travelling abroad are vulnerable to economic espionage due to the limited control they can exercise over the foreign business environment. In this context, a foreign government can operate more easily and with greater impunity in its own country. Hotel rooms, restaurants, office buildings, safes, telecommuni-cations systems and personnel are more vulnerable than domestic counterparts to compromise through covert economic espionage activities.

In one case, it was suspected that a host government was intercepting telephone conversations between an executive abroad and his Canadian company headquarters. Canadian executives discussed detailed negotiation information including a specific minimum bid. This minimum bid was the immediate counter-offer put forward by the host company the following day.

In another incident, an executive from a Canadian company, while visiting a foreign company overseas with which it had a business agreement, strongly suspected that his briefcase and documents had been compromised while they were left in the "security" of the foreign corporation's office.

Once again, if the potential gains are significant enough, any covert method or a combination of some of them can be used to acquire the desired information or technology, and obviously it is easier for a foreign government to initiate covert activities on its own territory.

Countries Involved

While some traditionally "hostile" countries continue to pose a threat to Canada's economic security, there are strong indications that other foreign governments - including some of those from countries considered "friendly" to Canada - use espionage as a means to further their economic and commercial

interests. Any competing nation, given sufficient motivation, may well engage in espionage against Canada to further its economic objectives.

2. The Protection of Valuable Information

National Liaison / Awareness Program

"Canadians are concerned about their sense of security in the world - a world that is ever more influencing our conduct at home in terms of the economy, jobs, protecting the environment and our democratic institutions".

The Hon. Herb Gray, former Solicitor General,

Statement on National Security, April 11, 1984

The Service established its National Liaison/Awareness Program in January 1992. The program seeks to develop an ongoing dialogue with organizations, both public and private, concerning the threat posed to Canadian interests by foreign government involvement in economic and defence-related espionage. The purpose of the program is to enable CSIS to collect and assess information that will assist it in its investigation of economic espionage activities against Canada. The Service then assesses the threat, and provides advice to government accordingly.

"What we have seen and witnessed, obviously, by the end of the Cold War is a change in the focus and targeting of foreign intelligence services. They put more emphasis on economic espionage and on acquiring scientific and technological information. Our response to that program was to do something that resembles a community interview program. We established a liaison program. We tried to determine what areas of Canadian industry are likely to be most targeted. Obviously it is in those technology areas like aerospace, nuclear, biochemical, and telecommunications in which we have a state-of-the-art and state-of-the-world industry".

Ray Protti, former Director of CSIS,

Standing Committee on Justice and Legal Affairs, May 3, 1994

The program is voluntary. It provides organizations with a better appreciation of the threat environment, and thus enables them to better protect themselves. Upon request, an Economic and Information Security (EIS) coordinator can provide an organization with formal presentations. CSIS has regional and district offices across the country.

Based on CSIS' experience in investigating foreign government espionage activities in Canada, the presentation includes a review of the most common covert methods used, as well as elements that businesses should consider in assessing their own vulnerabilities. CSIS does not provide a security consulting service, and cannot provide specific advice regarding steps a company needs to take to protect its proprietary information and technology.

Current Information on the Liaison / Awareness Program

Since its inception in 1992, CSIS' Liaison/Awareness Program has met with a positive response from the Canadian public and private sectors. Over the years, the Service has made thousands of contacts within Canadian industry and government.

Assessment of the Vulnerability

Companies are in the best position to determine what information or technology is critical to their business. Companies can assess what sensitive information could be targeted and can help determine from whom it must be protected. This principle applies to their operations in Canada, as well as business executives travels abroad.

The protection of sensitive information and technology is a matter of appropriate physical and personnel security, as well as an educational process. The following are some basic measures that, if implemented, can help reduce the vulnerability of companies to economic espionage:

Appropriate classification, control and protection of sensitive documents;

Protection of computer databases and network links from unauthorized access;

Proper storage and disposal of sensitive documents;

Discussion of sensitive company matters in appropriate locations;

Realistic controls on employees/visitors access to sensitive facilities, materials, etc., based on the "need-to-know" principle;

Sensitivity and caution with the choice of medium used for business communications (i.e. cellular telephones, open fax and telephone lines) and;

Education and sensitization of all employees to the threat that economic espionage may pose to job security and the organization's economic well-being. Emphasis on sharing responsibility amongst all employees for adherence to effective security policies and practices.

Contact

For comments/enquiries, please contact the National Coordinator, Economic and Information Security, c/o P.O. Box 9732, Postal Station T, Ottawa, Ontario, K1G 4G4. Telephone 613-231-0100 or fax 613-842-1390.

Definitions

economic security:

Economic security is the maintenance of those conditions necessary to encourage sustained long-term relative improvements in labour and capital productivity and thus a high and rising standard of living for a nation's citizens, including the maintenance of a fair, secure and dynamic business environment conducive to innovation, domestic and foreign investment and sustainable economic growth. This is a broad goal sought by all governments.

economic intelligence:

Economic intelligence is policy or commercially relevant economic information, including technological data, financial, proprietary commercial and government information, the acquisition of which by foreign interests could, either directly or indirectly, assist the relative productivity or competitive position of the economy of the collecting organization's country.

economic espionage:

Economic espionage is defined as illegal, clandestine, coercive or deceptive activity engaged in or facilitated by a foreign government and designed to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage.

industrial espionage:

Industrial espionage is the use of, or facilitation of, illegal, clandestine, coercive or deceptive means by a private sector entity or its surrogates to acquire economic intelligence.

ARCHIVED: Backgrounder No. 7 - Proliferation Issues

Backgrounder No. 7 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

Revised April 2003

"Despite the best efforts of our diplomats and counter proliferation experts, the spread of weapons of mass destruction will be a defining security challenge of this new century. It will lead to more fingers on more triggers. Not all of these fingers will belong to rational leaders. In such a situation, deterrents may not always deter." NATO: A Vision for 2012

Speech by NATO Secretary General, Lord Robertson

At the NATO/GMFUS Conference, Brussels, Belgium October 3, 2002

Introduction

The terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001 wakened people to a realization of the damage that an organized, motivated enemy could inflict on a civilian population. Less than a month after these attacks, news broke that several people had been infected by anthrax. Many immediately linked the two events and fears emerged that biological weapons were being employed by terrorists against American civilian populations. It was soon discovered that the mail was being used to send anthrax and the US Mail activities were interrupted as people feared opening their letters. The term "weapons of mass destruction" became part of the public's vocabulary.

In reality, the spread and potential use of weapons of mass destruction have been an issue for many years. In 1995, the Aum Shinri Kyo, a Japanese religious cult, released the nerve agent sarin in the Tokyo subway, killing 12 and injuring thousands. In 1998, India and Pakistan shocked the world with a series of nuclear tests that demonstrated the potential consequences of future conflict in the region. By May 2002, relations between the two countries over the disputed Kashmir region deteriorated to the point that a war, possibly involving nuclear weapons, appeared likely.

These episodes demonstrate how the proliferation of nuclear, radiological, chemical and biological weapons, commonly grouped as weapons of mass destruction (WMD), as well as their delivery systems, have the potential to undermine international peace and security.

In January 2001, the United States Department of Defense, in its document Proliferation: Threat and Response, estimated that at least 25 countries possess-or are in the process of acquiring and developing-capabilities to inflict mass casualties and destruction through nuclear, biological or chemical weapons or the means to deliver them. The Federation of American Scientists in 2000 placed the number of countries possessing, pursuing or capable of acquiring such weapons and/or delivery systems at 33. While many terrorist groups lack the resources, expertise or motivation to employ WMD, there has been a growing interest among certain terrorist groups in acquiring such weapons as well. Regardless of the exact number of parties seeking WMD or their delivery systems, such estimates demonstrate what a widespread and serious issue proliferation has become and the urgent and continuing need to counter this threat.

The Government of Canada is committed to countering the spread of such weapons. Canada is a party to various international agreements which seek to prevent the proliferation of weapons of mass destruction, their delivery systems and components which can be used to produce such weapons or systems. As Canada is an internationally recognized leader in many high-technology sectors (such as the nuclear, chemical, pharmaceutical, biotechnological, electronics and aerospace sectors), it remains a frequent target for clandestine and illicit procurement activities by countries of proliferation concern.

The WMD Threat

Nuclear and Radiological Weapons

Nuclear weapons are considered weapons of mass destruction in the truest sense. In addition to killing tens or hundreds of thousands of people or more, a nuclear weapon can destroy the entire physical structure of a large city and contaminate a much larger area with radioactive fallout. In addition to the five traditional nuclear weapons states (the United States, Russia, China, France and the United Kingdom), India and Pakistan have admitted their nuclear capabilities and Israel has long been credited with a clandestine arsenal. A number of other countries, including Iran, Libya, North Korea, and until recently, Iraq were widely suspected of harbouring nuclear weapons ambitions and/or to be actively pursuing such programs. Most analysts believe that the spread of nuclear weapons capabilities in general, and in particular to less stable or conflict-ridden regions of the world, would be harmful to international security by increasing the likelihood of nuclear weapons being used during wartime or serving as coercive tools in international diplomacy.

The basic concepts related to the development of nuclear weapons have been widely known for some time and the required technology dates back to the 1940s. However, the infrastructure required to produce nuclear weapons indigenously is considerably more difficult and expensive to develop than that for either biological or chemical weapons. This is one reason why concern about WMD terrorism focuses more on CBW than nuclear weapons.

The greatest obstacle to a potential proliferant is obtaining sufficient amounts of fissionable material (highly enriched uranium or plutonium). Countries with advanced nuclear weapons programs attempt to acquire technologies and components that can allow them to indigenously produce such fissionable material, often under the auspices of a civilian nuclear power program. Otherwise, they can attempt to purchase or steal weapons-grade fissionable material kept in scientific institutions having research reactors. It is estimated that approximately 20 tonnes of highly enriched uranium is stored in such locations throughout the world. The vulnerability of this fissile material to theft or misuse is a significant proliferation concern at the present time.

Technical complexities and expense reduce the likelihood that most terrorist groups could construct a nuclear explosive device. Theft of an intact nuclear weapon is also not considered very likely given the

stringent security measures in place in most of the nuclear weapons states. A more likely threat from a terrorist organization would be a radiological one involving the dispersal of radioactive substances to contaminate the air or water, or to render a particular area or facility unusable. Radioactive materials that could be used for such contamination are available from a wide range of relatively non-secure facilities, including hospitals, medical and research laboratories, universities and waste dumps. Although some types of contamination may be more difficult to achieve than commonly believed, given the widespread public anxiety about nuclear material in any form, the mere threat of such use of radioactive materials could be a potent terrorist tool.

Chemical and Biological Weapons

Chemical and biological weapons are particularly brutal tools of death and can kill slowly and painfully. Unfortunately, such weapons, particularly biological agents, are also easier and cheaper to produce than nuclear materials and the technology and know- how is widely available. As a result, there are far more states actively engaged in chemical and biological weapons programs than there are in nuclear programs. The Federation of American Scientists estimated that 29 nations possess, were pursuing or are capable of acquiring chemical or biological weapons as of 2000. These countries included Iran, Libya, North Korea, Syria and until recently, Iraq.

Chemical agents include blood agents, choking agents, blistering agents and nerve agents. Some chemical agents utilize toxic industrial chemicals and do not require much expertise to be adapted into potential weapons. Biological agents include bacterial, viral and rickettsial agents. An individual with some technical training could apply the necessary expertise given supplies and a basic laboratory to make a crude biological weapon. Certainly, any state with a modestly sophisticated pharmaceutical industry is capable of producing biological agents. Biological agents, in particular, could cause mass casualties if detection and treatment were impeded.

Fortunately, the frightening potential of biological and chemical weapons are mitigated by several factors, the most important being that it is very difficult to find effective, reliable delivery means for large-scale lethal doses of such agents. Many chemical agents require large quantities of precursor chemicals and can require high-temperature processes and create dangerous by products, making production outside of an advanced laboratory unlikely. If used, biological agents can be affected by environmental factors including wind, temperature and rain. Chemical agents are rapidly diluted when exposed to air. Also, immunization will not guarantee the safety of those who deliver the weapon. The amounts of agents needed also make large-scale food and drink contamination unlikely and make it very difficult to contaminate a large water supply, although smaller-scale contamination is possible. The

release of such chemical or biological agents through vaporizing or aerosol devices has to be in a confined area for lethal exposures to occur. This indicates that enclosed spaces such as urban transportation systems, sports stadiums and office complexes are more vulnerable to such attacks than other more open areas.

Delivery Systems

There are three types of delivery systems usually considered for WMD-ballistic missiles, cruise missiles and combat aircraft. Among these, the ballistic missile is the greatest proliferation concern both because it is difficult to defend against and because it appears to be particularly suited for WMD.

A ballistic missile has been defined as "a rocket-powered delivery vehicle that has some form of guidance system, that is primarily intended for use against ground targets, and that travels a large portion of its flight in a ballistic (free-fall) trajectory." While aircraft or cruise missiles might be better suited to deliver chemical or biological weapons, ballistic missiles may be ideal for delivery of WMD (biological, chemical or nuclear) against specific point targets or for terror attacks designed to intimidate a population. In general, compared to aircraft, ballistic missiles are harder to defend against, swifter in their delivery, and easier to hide from opposing forces. They may also be cheaper to acquire and maintain than modern types of combat aircraft. Precisely because they appear to represent the highest state of technological advancement and are less common than aircraft, their acquisition by a state may be considered particularly prestigious. Thus, it is no coincidence that virtually all states known to possess or suspected of developing WMD also maintain ballistic missile programmes.

Over a dozen states in addition to the five permanent members of the UN Security Council possess or are developing ballistic missiles with ranges of over 300 kilometres. Most of these counties also have active WMD programmes. These countries include India, Iran, Israel, Libya, North Korea, Pakistan, Syria and until recently, Iraq. Countries of proliferation concern vary widely in their ability to produce missiles, extend their capabilities or design new types. Practically all such states depend on assistance or at least purchases of supplies from abroad; outside the most industrially advanced states, only Israel, India and China can be considered truly independent in missile design and production.

Despite limited success in some instances, the Missile Technology Control Regime has proven unable to completely stem the proliferation of ballistic missiles and the number of states acquiring such missiles and their production capability will continue to grow. Of greatest concern is the situation in South Asia, where India and Pakistan appear to be involved in a nuclear ballistic missile "race" with potentially

severe consequences for regional and global security. The ballistic missile programs of some other states (such as Iran, Israel, North Korea, Syria) are also worrisome because they have acquired, or soon will have, the capability to deliver weapons of mass destruction against neighbouring states and foreign military forces within their respective regions and even, in some cases, beyond.

Canada's Role in Stemming the Tide of Proliferation

The Government of Canada firmly believes that the proliferation of weapons of mass destruction and their delivery systems poses a significant threat to international peace and stability. While the immediate threat of Canada being directly targeted for an attack with a weapon of mass destruction is low, Canadian troops serving in peacekeeping or peace-enforcement missions, as well as other Canadian citizens abroad, may be at higher risk of attack. As delivery ranges increase, some of Canada's allies are being rendered vulnerable to such attacks against their home territories. In the longer term, as proliferation increases, a few states potentially hostile to Canadian interests could acquire the capability to strike Canada directly.

Canada is party to a number of international treaties forbidding the transfer of weapons of mass destruction such as the 1970 Nuclear Non-Proliferation Treaty and the 1972 Biological and Toxin Weapons Convention. In addition, Canada was one of the original signatories of the Chemical Weapons Convention. However, these treaties have not deterred non-signatories and certain states that ignore their treaty commitments from attempting to acquire WMD materials and technology. Canada is also actively promoting the development of an effectively verifiable treaty banning the production of fissile material for nuclear weapons and other nuclear explosive devices and advocates an immediate and universal moratorium on the production of fissile materials for weapons and explosive purposes.

Canada is also a part of several international supplier regimes and cooperation agreements designed to control the transfer of WMD technology and materials to countries of proliferation concern through the strengthening of national export control measures. These include the Australia Group (chemical and biological warfare); the Nuclear Suppliers Group, also known as the London Club (nuclear weapons and related dual-use technology); the Missile Technology Control Regime (missiles and unmanned aircraft capable of delivering weapons of mass destruction); and the Wassenaar Arrangement (transfer of conventional arms and dual-use goods and technologies).

Canada's technological leadership makes it a potential source of expertise, materials and technology for states pursuing WMD or ballistic missile programs. As a result, Canada remains a target for clandestine

and illicit procurement activities by countries of proliferation concern. In addition, Canada is a major world supplier of uranium and nuclear power technology. Plutonium from a Canadian-supplied reactor was used in India's first nuclear explosion. It would be highly embarrassing to Canada if Canadian-produced expertise, materials or technology were again used by a state to produce weapons of mass destruction or their delivery vehicles.

The Mandate and Role of CSIS

In response to these threats and the government's security intelligence priorities, the Service has refocused its operations to create a more intensive, strategic investigative effort against proliferation and ensure timely advice is provided to the government on this threat to national security. In July 2002, CSIS created the Counter Proliferation Branch, which combines the expertise of both the counter-intelligence and counter-terrorism fields to address the merging threat of weapons of mass destruction.

The branch fulfills its role, within the CSIS mandate, by collecting information related to biological, chemical and nuclear weapons development programs undertaken by foreign governments or terrorist organizations. Through exchange relationships with foreign governments and by working closely with federal government departments and agencies, including the Department of Foreign Affairs and International Trade, the Department of National Defence, the Canada Customs and Revenue Agency, the National Research Council and the Canadian Nuclear Safety Commission, the branch is able to expand upon and share its knowledge about threats and emerging trends in the area.

The changing face of terrorism has made the potential use of chemical, biological, radiological or nuclear weapons in a terrorist attack a reality. A recent case involving ricin in the United Kingdom demonstrates how easy it is to produce biological agents. Instructions are readily available on the Internet. Anyone with an undergraduate knowledge of chemistry has the skill to produce them. Since the terrorist attacks on September 11, 2001, Service investigations into the terrorist use of weapons of mass destruction have been expanded. The Service monitors all information regarding terrorist interest in acquiring such weapons.

The primary objective of CSIS investigations is to forewarn government of threats to national security. With the information it gathers, the Service develops assessments of potential WMD threats within Canada or against Canadian interests, which are distributed to the broader security and intelligence community and to other federal government departments and agencies. In addition, the Service works closely with other government departments and law enforcement agencies to counter these threats.

Conclusion

The proliferation of chemical, biological, nuclear and radiological weapons and their delivery systems is one of the most important security intelligence challenges facing CSIS today. The challenge is evolving as more is learned about the progress being made by foreign countries in their weapons development programs and as certain terrorist groups begin to covet the power and destructive force these weapons represent. Through its dedication to its mandate, CSIS has a vital role to play in ensuring that, to borrow from the comments of the Secretary General of NATO, we limit the number or triggers and the fingers on those triggers.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

ARCHIVED: Backgrounder No. 8 - Counter-Terrorism

Backgrounder No. 8 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

Revised June 2007

The Service's number one priority

Ensuring the safety and security of Canadians is one of the Government of Canada's most important responsibilities. With this in mind, the government has identified counter-terrorism as the Canadian Security Intelligence Service (CSIS) number one priority.

What is CSIS' counter-terrorism role?

The Service's role is to: forewarn and advise the Government of Canada of potential threats, with the goal of preventing terrorist acts from being planned and/or carried out in Canada and from affecting Canadians abroad. It does this by investigating, collecting and analysing information and providing timely information and advice to law enforcement and government decision-makers.

Are terrorists active in Canada?

Like many other Western democracies, Canada has its share of individuals who support the use of violence to achieve their political goals. Their activities are often linked to conflicts around the globe and typically include: planning or helping to plan terrorist attacks in Canada or abroad; providing a Canadian base for terrorist supporters; fundraising; lobbying through front organizations; obtaining weapons and matériel; finally, coercing and manipulating immigrant communities.

Canada has not been immune to the more recent phenomenon of "homegrown terrorism," which refers to the sometimes rapid indoctrination and radicalization of young Canadians into the violent ideology espoused and inspired by Al Qaida.

Canada is also home to individuals and groups that support the use of violence to achieve domestic political goals. These individuals and groups work outside the legitimate political system.

What is the Service's priority investigation?

CSIS' current counter-terrorism priority is the threat posed by individuals and groups inspired by the ideology of Al Qaeda.

As an open, democratic and multicultural society, Canada attracts hundreds of thousands of legitimate immigrants and refugees from all corners of the world. Our country's openness and respect for human rights also make it attractive to members of terrorist organizations bent on using Canada as a base to support their activities.

International terrorist groups have been active in Canada for years but, more often than not, they were engaged in support of activities such as fundraising or acquiring matériel and equipment.

In the last decade or so, the threat has evolved, and Canadians and Canadian interests at home and abroad are at increased risk. Canadian citizens or residents have been involved in terrorist attacks or planned attacks in Canada or abroad, or have been victims of terrorist activity outside of Canada.

What legal tools are used to counter terrorism?

CSIS operates under the authority of the CSIS Act, which provides a legal mandate to investigate individuals or organizations suspected of involvement in political violence and terrorism, regardless of where the threat to Canadian security originates. Although CSIS is not a law enforcement agency, and has no powers of arrest or detention, it works closely with law enforcement agencies across Canada to strengthen public safety.

The Royal Canadian Mounted Police (RCMP) and other police forces use the Criminal Code and the Anti-terrorism Act. The Anti-terrorism Act provides measures to deter, disable, identify and prosecute those involved in terrorist activities or supporting such activities, and makes it an offence to knowingly support terrorist organizations, whether through overt violence, or by providing support through documentation, shelter or funds. CSIS has no authority under the Anti-terrorism Act.

CSIS works to ensure that:

Canada is not a place where people are killed or injured by terrorism;

Canada does not provide a base for terrorists to plan acts of terrorism, either in Canada or abroad;

Canadian institutions are protected; and

Canadians travelling or working abroad – including members of the Canadian Forces – are protected.

What are CSIS' primary counter-terrorism activities?

Investigations

In the course of CSIS investigations into threats to the security of Canada, the Service relies extensively on the voluntary cooperation of members of the public. CSIS may use surveillance to monitor the activities of individuals of interest. The Service may also obtain Federal Court warrants which allow the use of other investigative techniques.

Threat Assessments

The Integrated Threat Assessment Centre (ITAC), housed at CSIS Headquarters, is a government centre staffed by representatives from government departments, agencies and police forces. ITAC produces comprehensive, integrated threat assessments, which are distri-buted within the intelligence community and to relevant first-line responders on a timely basis. These assessments allow the Government of Canada to more effectively coordinate activities in response to specific threats in order to prevent or mitigate risks to public safety.

Security Screening

Under its Government Screening Program, CSIS provides security screening services to federal departments and institutions. The Service also performs "site-access" assessments of individuals seeking employment at airports and nuclear power stations and in the federal parliamentary precinct. The Service thus helps to ensure that individuals with terrorist connections do not obtain access to our country's sensitive sites or classified information.

CSIS screens immigrant applicants, providing Citizenship and Immigration Canada (CIC) with in-depth examinations of prospective immigrants whose backgrounds may present security concerns, and provides front-end screening of refugees to identify terrorists posing as refugee claimants wishing to enter into the country.

Assisting law enforcement and immigration officials

The CSIS Act gives CSIS the authority to share information with the RCMP and other police authorities to assist them in their criminal investigations. The June 2006 arrests of 17 individuals in the Toronto area were the result of an RCMP investigation based on CSIS lead information CSIS also provides input to the Canada Border Services Agency's Enforcement Information Index, an automated system that alerts immigration and customs officers abroad and at ports of entry about security threats posed by suspected and known terrorists seeking admission to Canada. CSIS information enables Canadian immigration officials to refuse applications from individuals suspected of involvement in terrorist activity, effectively barring their entry into Canada.

Liaison and cooperation

In Canada, CSIS works closely with other government departments and law enforcement agencies at the federal, provincial and municipal levels to respond to terrorist threats and incidents.

The CSIS Act allows the Service to enter into an arrangement with a foreign agency, only after the Minister of Public Safety, in consultation with the Minister of Foreign Affairs, have approved the arrangement. Currently, the Service has about 270 cooperative relationships with more than 145 countries, giving it access to global information and intelligence on potential terrorist threats.

Advice to government

The primary goal of intelligence-gathering is to provide timely and accurate information, analysis and advice to government policy-makers through detailed reports, studies and briefs on issues related to terrorism and public safety. CSIS tactical analysis combines intelligence gathered by the Service with information from other sources, including government agencies and other intelligence services, while its strategic analysis offers comprehensive, policy-relevant intelligence assessments to government.

Terrorist listings

Under the provisions of the Anti-terrorism Act (ATA), CSIS may provide advice to the government with respect to the listing of terrorist entities. The consequences of being a listed entity are severe: first, the listing process is public; second, a listed entity is automatically considered a 'terrorist group' by definition, and the Criminal Code clearly spells out the sanctions for those dealing with a terrorist group; and third, the assets of a listed entity may be immediately frozen.

Since the creation of the list, CSIS has contri-buted to listing 40 entities, including Al Qaida the Liberation Tigers of Tamil Eelam and Hizballah, groups which have operated or had supporters in Canada for many years.

The United Nations (UN) also maintains several lists of designated terrorist entities. Much as with the ATA list, the immediate result of being listed pursuant to the UN regulations is public identification as being associated with terrorism, an automatic freeze of assets and prohibition of any fundraising efforts. CSIS' role is to provide advice to the Department of Foreign Affairs and International Trade, which is ultimately responsible for Canada's international obligations with respect to UN resolutions.

Human rights vs. national security—Finding the balance

CSIS is considered by many to be the most externally reviewed security intelligence service in the world. In fact, the CSIS Act, enacted in 1984, served as the model for subsequent legislation for the Australian and British security services

CSIS operates within a strong legal framework, which allows the Service to carry out its activities while concurrently protecting the civil liberties of individual Canadians.

Ministerial direction sets clear limits on how the Service undertakes investigations. For example, the use of human sources on a post-secondary campus is strictly regulated and must be approved by the Minister of Public Safety.

Intrusive investigations are subject to senior-level approval. When warrant powers such as intercepts are required, the Minister and a special designated judge of the Federal Court of Canada must authorize them.

While CSIS may enter into arrangements with foreign countries and agencies, it may only do so with the approval of the Minister of Public Safety in consultation with the Minister of Foreign Affairs. Any information shared with those foreign agencies is accompanied by various caveats restricting both the use and further dissemination of that information. CSIS has also developed a new caveat, which seeks assurance that any Canadian citizen detained by a foreign government will be fairly treated within the accepted norms of international conventions, and that he is accorded due process under law and afforded access to Canadian diplomatic personnel, if requested.

Furthermore, the Security Intelligence Review Committee (SIRC) has the mandate to review the Service's operational activities, to assess whether the Service's actions have been carried out in accordance with the laws of Canada, directions from the Minister and CSIS operational policy and to inform Parliament and the Canadian public.

Of course, like all federal agencies, CSIS is also subject to Government of Canada laws and regulations. The Service has been audited by the Auditor General's Office; complies with the Access to Information Act and the Privacy Act; has appeared before the Canadian Human Rights Commission to respond to complaints; and has testified at public proceedings including the O'Connor Commission into the Actions of Canadian Officials in Relation to Maher Arar and various Federal Court hearings.

The full spectrum of legal and institutional mechanisms in place ensures that CSIS does its work in a way that respects individual liberties, while maintaining its ability to investigate potential threats to the collective security of this country.

ARCHIVED: Backgrounder No. 9 - Security Screening

Backgrounder No. 9 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

November 2004

The Security Screening program is one of the main operational responsibilities of Canadian Security Intelligence Service (CSIS). The goals of the program are to prevent non-Canadians who pose security concerns or risks from entering or receiving permanent residence in the country and to prevent anyone of security concern from gaining access to sensitive government assets, locations or information. The Security Screening Program is one of the most visible functions undertaken by CSIS.

The September 11th tragedy in the United States has refocused attention on the requirement for good security screening procedures throughout the Government of Canada. In the December, 2001 budget, the Government of Canada announced substantial increases in funding for CSIS over the next five years. Much of this increased budget has been earmarked towards both government and immigration screening programs.

On behalf of the Government of Canada, CSIS security assessments fall into three main program categories: Government Screening, Foreign Screening and Immigration and Citizenship Screening.

Government Screening

The Government Screening Program provides security assessments for all government departments and institutions, with the exception of the Royal Canadian Mounted Police. The Service also has a site access program for airports, the Parliamentary Precinct and nuclear power stations. These programs assist in enhancing security and reducing the potential threat from terrorist groups and foreign governments which seek advantage from gaining access to classified information or other assets and materiel. Since September 11, the demand for CSIS advice has risen dramatically.

The majority of Government Screening resources are devoted to federal government departments. Under the Government Security Policy (GSP), federal employees, members of the Armed Forces or persons under contract to a government department who in the performance of their duties have access to classified government assets or information, are required to hold security clearances.

There are three levels of security clearance as defined by the GSP: Confidential (Level I), Secret (Level II) and Top Secret (Level III). The level of security clearance required is determined by the need for access to classified information or assets in the performance of duties associated with an individual's employment.

Level I and II security clearance requests, which are conducted electronically, require checks in CSIS data banks. Most result in a recommendation to grant the clearance being made to the Departmental or Agency Security Officer (DSO/ASO). Further enquiries including an interview with the subject or a full field investigation may be required at times, if the process reveals questionable information. A full field investigation is required for all Level III security clearances.

A field investigation includes CSIS records checks, the interview of friends, neighbours and employers, local police checks and possibly an interview of the applicant. During the course of the enquiries, every effort is made to explain the purpose of the questions being posed and participation in the interviews is voluntary.

The security screening process may reveal significant information which would lead CSIS to recommend that the requested clearance be denied. In other cases, CSIS may advise the DSO/ASO of information which, while being of concern, may be insufficient to warrant a recommendation to deny, but would nevertheless require departmental attention and appropriate action. While the Service assists the

originating department by providing an assessment of the individual's reliability and loyalty to Canada, under the GSP, all departments have exclusive authority to grant or deny security clearances.

In 2003-2004, CSIS received 37,327 requests for site and airport access. A total of 37,508 security clearance requests were received for government departments and agencies including the Department of National Defence (DND). For areas of the federal government, other than DND, the median time required to process Level I applications was seven days. Level II applications required 11 days to process while Level III took 82 days. Times required for DND were 20, 18 and 96 days respectively.

Foreign Screening

CSIS has reciprocal screening agreements with the governments of foreign states, foreign agencies and international organizations which provide them with security assessments. These agreements are all approved by the Minister of Public Safety and Emergency Preparedness after consultation with Foreign Affairs and International Trade Canada.

All persons affected by this procedure provide their agreement in advance. The requests for foreign screening typically fall within two categories: database checks and enquiries on Canadian residents wishing to take up residence in another country; or field checks and enquiries on former and current Canadian residents who are being considered for classified access in another country.

In 2003-2004, the Service received and processed 1,208 requests for security assessments in its Foreign Screening Program.

Immigration and Citizenship Screening

The provision of security advice in immigration and citizenship matters is crucial to countering imported threats to the security of Canada. The screening program serves as a first line of defence against those who attempt to penetrate the country to undermine Canadian security.

Working closely with Citizenship and Immigration Canada (CIC), the Service's Immigration Screening program's primary task is to provide security-related advice to CIC. The objective is to prevent persons who are inadmissible under the Immigration and Refugee Protection Act (IRPA) from entering or gaining status in Canada.

One important change, that has been introduced in the past few years, from a security screening point of view, is the adoption of Front End Screening (FES) for all refugee claimants to Canada. FES is a government initiative to ensure that all refugee claimants arriving in Canada are checked against CSIS and RCMP records before they are sent to the Immigration and Refugee Board. The initiative was implemented to identify and filter potential security and criminal cases from the refugee claimant stream as early as possible in the determination process. Prior to FES, CSIS did not screen refugee claimants.

In addition to its new responsibilities for Front End Screening, the Service, for many years, has had the responsibility for conducting security screening of immigrants and refugees who apply for permanent residence status from both within Canada and outside Canada. CSIS provides advice to the Minister of Citizenship and Immigration related directly to the security inadmissibility criteria contained in the Immigration and Refugee Protection Act. CSIS also provides CIC with security assessments on applicants for Canadian citizenship. CIC forwards all applications for citizenship to CSIS for review. The Service advises if any security concerns relating to a particular application surfaced in the course of its checks, and provides CIC with relevant security advice if such concerns come to light.

The use of information technology has greatly assisted in reducing the time needed to process requests from CIC. In 1996-1997, the Service began to receive its trace requests related to citizenship applications through an Electronic Data Exchange directly from CIC's Case Processing Centre in Sydney, Nova Scotia. Beginning in November 2001, CIC has also made available an input process for all immigration officers in Canada, enabling CIC front-line officers to send data to CSIS electronically, greatly facilitating the front end screening process. Screening requests for immigrants applying to CIC from within Canada are now all conducted electronically between the Service and CIC. Requests related to immigrants applications from outside of Canada traditionally took longer to process since such applications were sent to the Service on hard copy forms and mailed via diplomatic bags. However, electronic exchange systems installed at posts abroad have significantly reduced turnaround times. CSIS is also increasing the number of liaison officers abroad to further improve processing of these applications and reduce existing backlogs.

Over the fiscal year 2003-2004, the Service received some 44,907 requests for Immigration Screening from within Canada (including RDP) and issued 46,183 security clearance assessments. Additionally, the Service received some 24,243 Immigration Screening applications from outside Canada and 4,646 from the United States for a total of 73,796 immigration cases. The median turnaround time was 42 days (through the Electronic Data Exchange Program) for requests from within Canada. Under the Overseas Program, our Security Liaison Officers were consulted on 4,814 cases.

Citizenship Screening is conducted on the basis of threats to Canada's security as set out in s.19 of Citizenship Act. Over the past years, 203,356 citizenship requests were received from Citizenship and Immigration Canada.

The Front End Screening

The FES program, implemented to identify and filter potential security cases from the refugee claimant stream as early as possible in the determination process, received 22,681 cases over the past year.

ARCHIVED: Backgrounder No. 10 - Transnational Criminal Activity

Revised March 2003

"Combatting organized crime is the number one law enforcement priority on Canada's public safety agenda.

The Hon. Lawrence MacAulay, former Solicitor General, News Release, April 15, 2001

"The RCMP have the lead Federal role for combatting crime, but I believe that the increasing threat of transnational crime - notably the illegal traffic of drugs, people and the laundering of money across international boundaries - means that the RCMP and CSIS have to marshal all their resources in a cooperative and integrated fight against these activities.

CSIS specifically has a role to play by exchanging information with other countries and providing relevant criminal information and strategic analysis to Canadian law enforcement agencies."

The Hon. Andy Scott, former Solicitor General, Speech to the Throne, 30 April 1998

Introduction

Improvements in transportation, computer and communications technology have made the world today much smaller than it was 50 years ago. Intercontinental travel which used to require days or weeks now takes place in hours. The formerly daunting notion of conversing or conducting business with someone halfway around the globe is now a mouse-click or a telephone call away. This globalization has created a world virtually devoid of national borders. Unfortunately, these changes have also made it easier for members of highly sophisticated and organized criminal syndicates to pursue a complex Web of lucrative legal and illegal activities worldwide.

UN estimates place the cost of this transnational criminal activity in developed states at two per cent of annual gross national product (GNP). The potential transnational crime-related losses for Canada in 1995 would have been about $14.8 billion, based on a GNP of $742 billion. Figures like this led the 1998 G8 summit in the UK to label transnational criminal activity one of the three major challenges facing the world today.

Transnational crime threatens various aspects of Canadian national security, law and order, the integrity of government programs and institutions, and the economy. Accordingly, the Canadian Security Intelligence Service monitors such activity under its mandate to investigate foreign- influenced activities detrimental to Canadian interests, as set out in Sections 12 and 2 (b) of the CSIS Act, in order to provide strategic advice to government on how to deal with this immense problem. Given the global nature of transnational crime, the Service's work in this area includes a great deal of cooperation with law enforcement agencies and other intelligence services.

The New Brand of Organized Crime

In the past, crime syndicates were traditionally involved in illegal activities such as drug trafficking, prostitution, illegal gambling, loan-sharking and extortion. These organizations generally controlled specific territories, did not usually attempt to operate outside their spheres of influence and only rarely cooperated with other syndicates. In the 1950s for instance, a Sicilian mafia family in Palermo would require permission to operate, however briefly, in another family's zone even if that zone were only a block away.

Today, organized crime is no longer limited to street-level activity. Contemporary organizations are adaptable, sophisticated, extremely opportunistic and immersed in a full range of illegal and legal activities. While still involved at the lower level with drug trafficking, prostitution, loan- sharking, illegal gambling and extortion, they have expanded their activities to a quasi-corporate level where they are active in large-scale insurance fraud, the depletion of natural resources, environmental crime, migrant smuggling, bank fraud, gasoline tax fraud and corruption. In addition, their frequent use of money earned from their illegal ventures to fund legitimate ones allows them to launder money and earn even more profits. They apply many of their criminal tactics in these legal business operations, never hesitating to use violence or murder to get ahead. By way of illustration, the media have taken note of the deaths of a "surprising number" of people who opposed a campaign by a company-believed to be affiliated with a Russian/Eastern European transnational criminal organization-to gain control of 40 per cent of Russia's aluminum trade. Transnational criminal syndicates are not afraid to work globally in any

country where legal or bureaucratic loopholes allow them to take advantage of the system. As with international corporations, these organizations are quite willing to work together, often bartering for the use of each other's unique talents to accomplish specific tasks, or to make longer-term arrangements when it suits their needs.

The Major Players

There are approximately 18 active transnational criminal organizations represented in Canada, including Asian triads, Colombian cartels, Japanese yakuza, Jamaican posses, Mafia groups from the USA, Calabria and Sicily, Russian/Eastern European mafiyas, Nigerian crime groups and major outlaw motorcycle gangs. In recent years, a great deal of media attention has been paid to Russian/Eastern European based organizations.

Organized Crime in Russia and Eastern Europe

Organized crime in Russia and Eastern Europe began in the 17th century, the days of the select group of criminals known as the vory v zakone, the Thieves in Law, who controlled the criminal underworld. The vory existed only to steal and rejected legitimate society entirely. Most of the Thieves in Law were imprisoned in the gulags during the Soviet era, but they came back to thrive in the chaotic atmosphere that followed the lifting of the Iron Curtain in 1991. Today, these older criminal fraternities are joined by the new and younger "bandit" organizations which are concerned only with profit, and not the thieves' code.

Although estimates vary widely, it is generally accepted that 5,000 to 8,000 criminal organizations with as many as 100,000 members control between 25 and 40 per cent of Russia's GNP. The Russian Interior Ministry (MVD) estimates that these organizations control 40 per cent of private businesses, 60 per cent of state-owned enterprises and between 50 and 80 per cent of banks in Russia. According to the MVD, approximately 300 Russian and Eastern European organized crime groups operate transnationally in various areas, including extortion, fraud, murder, illegal gambling, loan sharking and alien smuggling. Four key areas, however, form the foundation of their global criminal power: narcotics trafficking, illegal arms dealing, money laundering and the export of Russian natural resources.

The Threat

Given that they attack the very fabric of life in a democratic, law-based society like Canada, the illegal actions of transnational crime organizations threaten law and order, directly affecting people's sense of security, trust, order and community-the very underpinnings of Canadian society. They regularly attempt to corrupt public officials with large amounts of money, thereby jeopardizing the integrity of government programs and institutions and forcing governments to spend more of their shrinking budgets on enforcement. Adding to the increased enforcement expenditures and the burden on the criminal justice system is the fact these activities often result in social costs with long-term effects, e.g. drug dependency and a rise in violent crime.

Transnational crime also poses a serious threat to the economic security of the nation in that its basic activities could undermine the workings of the free market economy. Due to their illegal activities, transnational crime groups have access to huge sums of money, which needs to be "washed." This large-scale money laundering has an impact on the operations of legitimate financial institutions that, in the long term, can go beyond the business sector with negative effects on the investment climate, tax revenues and consumer confidence. Moreover, these large amounts of money, combined with a willingness to use violence, enables transnational crime organizations to bribe, extort or coerce employees of financial institutions and governments.

International and Canadian Efforts

At their Summit in Birmingham, England in 1998, the G-8 leaders vowed to continue the fight against the world-wide problem of transnational crime which, they declared, threatens "to sap (economic) growth, undermine the rule of law and damage the lives of individuals in all countries of the world."

In May 1998, the Solicitor General of Canada stated:

"Because of organized crime's many manifestations and because it transcends our borders, it... calls for innovative, international co-operation... No single person, no single country can stop the daunting flow of transnational crime."

In August 1998, he reiterated the government's commitment to combat these activities, stating:

"To fight the menace of organized crime, we need nothing short of a strategic partnership between the federal government, the provinces, the territories, and the police community, so that we can bring our combined weight to bear. If we succeed, we will have forged a partnership unprecedented in Canada, and will take the fight against organized crime to an entirely new level."

Canada has been working in the G-8, the United Nations and the Organization of American States to develop and promote international standards. On May 14, 2002, the Canadian government ratified the United Nations Convention against Transnational Organized Crime (TOC) signed in December 2000. The TOC Convention, and its related protocols on migrant smuggling and trafficking in women and children, provides all countries with a shared framework and legal tools to enhance international cooperation.

Cooperation at the interdepartmental, intergovernmental and international levels is needed to fight these transnational crime organizations which work outside the rules, can be ruthless in carrying out their policies and are not democratically accountable for their behaviour.

The Role of CSIS

Law enforcement agencies in Canada have the lead role in the fight against transnational crime. For this purpose, they collect both tactical and strategic intelligence. Tactical intelligence is a primary concern of law enforcement as it is operational in nature and is geared towards action in the field, leading to arrests and prosecutions. The collection of strategic intelligence, however, is also important for Canada's police agencies. This type of intelligence is long-term in nature, provides a comprehensive view of a threat environment, assesses the extent of the threat and points out which areas are at risk-all of which allows law enforcement to advise government and to be pro-active in its efforts against transnational crime.

It is in the area of strategic intelligence that CSIS has a role to play. Many criminal groups with transnational capabilities pose a threat to Canadian national security, undermining many of Canada's strategic interests. If undeterred, these threats can manifest themselves in higher health and welfare costs associated with the consumption and trade in illegal drugs, the erosion of the Canadian tax base through lost revenues due to non-reported, illegal business activities, the undermining of Canadian law and sovereignty, and the erosion of public confidence in Canadian government institutions and the Canadian business community. The Service also cooperates with other democratic governments which have tasked their intelligence services to help combat this threat and exchanges information with allied intelligence agencies.

It is through this collection and subsequent analysis that the Service fulfills its mandate to provide the Government of Canada with strategic intelligence on threats to Canada's national security in this instance, the extent and nature of transnational crime in Canada. The Service's collection of strategic intelligence can also have an important benefit for law enforcement agencies, as CSIS is often able to provide them with timely, "spin-off" tactical information.

The Service created a Transnational Criminal Activity unit in January 1996, as part of a government- wide effort to combat this threat. This unit draws on the Service's operational and strategic analysis resources in order to collect intelligence related to transnational crime.

Trends in Transnational Crime

Cyber-crime has already emerged as a proven weapon in the arsenal of transnational criminal organizations and it is expected to play a bigger role in years to come. The growth of global, computerized financial networks has allowed these organizations to launder the profits of their illegal ventures quickly and easily through transactions that are instantaneous and virtually untraceable. The United Nations estimates that at least $200 billion in drug money is laundered every year largely via international electronic bank transfers. An estimated $3 billion to $10 billion is laundered in Canada every year.

It is also believed that transnational criminal organizations have, or soon will have, the capability to use computers for a multitude of other illegal activities: for instance, "hacking" or "cracking" into the computer systems of corporations, accessing valuable information and then extorting the corporation by threatening to destroy the data. More conventional than cyber-extortion, cyber- theft will continue to be a problem.

Legitimization is another trend among transnational criminals. Some are attempting to distance themselves from the illegal aspects of their operations by involving themselves in legitimate business ventures which are funded by the almost bottomless profits acquired through their criminal activities. Others seek civic legitimacy by making donations to community hospitals, charities, universities and political parties. They also try to have their photographs taken with high-ranking government officials or other high-profile personalities.

Cooperation among transnational crime organizations, already a major factor in the new world order of crime, is expected to continue and expand. Partnerships, bartering arrangements and alliances, either short or long term, allow these syndicates to better evade law enforcement agencies, to share existing infrastructure and to improve risk management.

Sophistication, already a quality of transnational crime, is expected to increase. For instance, some members of transnational criminal organizations have university educations in the fields of business, accounting and law, better equipping them for the complex world of transnational crime.

Outlook

Given their sophistication, adaptability and opportunism, transnational crime organizations will likely continue to pose a threat to Canada's national security. Their wide-ranging activities have far-reaching detrimental effects on Canada's system of government and way of life.

Given their long history of survival and the successful nature of their operations in Canada, it is believed these organizations will continue and likely expand their activities here, further challenging Canadian social, political and economic institutions, as well as those elsewhere in the world.

In order to minimize the threat to Canada's national security from this challenging global threat, the Service will continue to investigate and report on the activities of foreign-based transnational criminal organizations in Canada.

ARCHIVED: Backgrounder No. 11 - Information Operations

Backgrounder No. 11 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

Revised February 2004

Introduction

With the advent of the personal desktop computer in 1980, the manner in which the public and private sectors conduct business and provide services to the public at large has changed. Over time, millions of computers and thousands of dissimilar networks worldwide have been connected through a global network of networks. Internet use has more than doubled annually for the last several years to an estimated 40 million users worldwide in nearly every country today. Connections between computer systems are growing at an ever-increasing rate, with the Internet adding a new network about every 30 minutes. According to a report by the Computer Industry Almanac, nearly 43 percent of Canadians use the Internet, which makes Canada the leading country for Internet use.

The growing dependence of governments, institutions, business, groups and individuals on computer-based communications and information technologies has resulted in a constantly changing view of what constitutes threats in today's "information age". It is no longer necessary for "hostile actors" (individuals, extremist and terrorist groups, intelligence services and armed forces) to directly access a computer to copy, destroy or manipulate data. People can use a variety of techniques and software tools to exploit a targeted system once they gain unauthorized access remotely via the Internet or by

dialling directly into the system using a telephone and a modem. Most legislation and protective measures address physical attacks on critical systems and data; however, they have been or are in the process of being revised and updated to deal with the new class of computer-based threats defined as Information Operations (IO).

Information Operations

The concept of IO has its root in that of "Information Warfare" (IW), which is the physical and computer-based operations used by military forces to compromise the access to and viability of information received by the decision-makers of an enemy, while at the same time protecting their own information and information systems. The term "Information Operation" (IO) is used to denote the use of IW tools and techniques at any time. The definition has evolved to reflect the need for a state to maintain national security by protecting its critical information infrastructure (CII). The eight critical sectors in a state's infrastructure include: transportation; oil and gas; water; emergency services; continuity of government services; banking and finance; electrical power; and telecommunications.

IO is the outgrowth of military doctrine that focussed on the use of electronic warfare measures to degrade the capabilities of adversaries on the battlefield. Operations conducted during the Desert Storm campaign indicated that technological development had provided the military with computer-based tools and techniques that could be used to degrade not only military systems but those of government and the private sector as well.

Within the realm of IO, there is no safe haven; territorial boundaries become irrelevant as IO can be conducted at any time against any sector (public or private). All other "cyber" activity (cybercrime, cyberterrorism, cyberwar, netspionage, hacktivism, etc.) is a subset of IO. However, most discussions relating to the use of computer-based tools and techniques in the context of IO have come to focus on information assurance and the protection of computer-based systems and networks from an intrusion or attack.

The Threat

Information Operations could be used to target national information systems from anywhere in the world using inexpensive hardware and software. Degradation in the operation of a targeted computer system could cause significant social, political and economic impact that would have serious

ramifications in the area of national security. Although security measures are being created to protect these infrastructures, the development of attack tools to circumvent these protective measures is ongoing and such attack mechanisms have come to be freely available through the Internet. The number of intrusions into computer-based systems is on the rise and the tools used to exploit existing vulnerabilities are growing in sophistication. Although only a small number of system intrusions are reported, indications are that the level of reported incidents and vulnerabilities is doubling roughly every six months. In 2000, statistics released from the Computer Emergency Response Team (CERT) at Carnegie Mellon University in Pittsburg show that 1,334 computer security incidents were reported world-wide in 1993, compared to 9,859 in 1999 and, in the first three quarters of 2000, the number of incidents rose to 15,167.

The threat of unauthorized intrusions into computer systems and networks increases proportionately to the degree of connectivity to external networks such as the Internet. Such connections create vulnerabilities that can be exploited, for whatever reason, by hostile actors, using malicious software, e.g. viruses, Trojan Horses and worms via the Internet. In addition, physical attacks like cutting power cables or destroying hardware upon which the information infrastructure depends are the equivalent of physical denial of service (DoS) attacks. The latter prevents authorized users from gaining access to information systems and data. Any of these hostile actors can attack vulnerable infrastructure points using physical means and/or software. As a result, the growing capability of a variety of hostile actors to make offensive use of IO, in both its physical and nonphysical forms, can potentially threaten the public safety of Canadians and the national security of Canada.

This is especially true since international affairs, in all their dimensions, will increasingly involve competition for control of information networks. Discussions at the United Nations on the topic of the proliferation of IO tools are couched in the rhetoric of weapons proliferation. The language has evolved from mass destruction to include IO tools and weapons of mass corruption. The increasing reliance of states on computer networks makes critical infrastructures attractive targets for attack and exploitation, and many countries have embarked on programs to develop IO technologies. According to American military and congressional reports, Russia, China, India and Cuba have acknowledged preparations for cyberwar and are actively developing IO capabilities; North Korea, Libya, Iran, Iraq and Syria have some IO capabilities. Even though many countries are developing IO capabilities, few have the means to fully integrate various IO tools into a comprehensive attack which would cripple a country's infrastructure. However, some could develop the required abilities to mount such attacks over the next decade.

Security of Systems and Data

The development of IO tools and techniques is evolving in pace with the rate of technological change in the communications and computer industries. The ability to communicate and connect with networks worldwide almost instantaneously has created both advantages and vulnerabilities.

As government departments and businesses globally have experienced both intrusions into their networks and the loss of sensitive information, they have attempted to install security measures to protect both systems and data. Unfortunately, these security packages have a short life span. Surveys and intrusion assessments conducted by private-sector security firms and by government agencies worldwide indicate that a large number of security packages and monitoring tools, many of which are commercially available, are ineffective or misused. A number of surveys conducted in the United States and the United Kingdom indicate that more than 80% of respondents in one case did not use firewalls or any other security measures to protect their systems and data. Up to 93% of respondents in another case were vulnerable to rudimentary attacks even if firewalls were used.

As more and more persons, businesses and government departments become dependent on computer-based communications and the operations of interconnected networks, the configuration of interacting computer networks and operating systems becomes more complex and creates vulnerabilities. Natural forces (like storms), the natural evolution of network processes, and IO tools could pressure these vulnerabilities and cause failures that could have a profound effect, both short- and long-term, on the operation of government and the private sector. For example, during the 1998 ice storm in Quebec and eastern Ontario, the destruction of the essential electrical power infrastructure cascaded into a disruption of key services such as water supply, financial services, telecommunications and transportation, with devastating consequences for some Canadians.

Examples of Information Operations

Many examples of IO-related activity can be drawn from the experience of American government departments dealing with computer intrusions and system exploitation. These experiences have been related in speeches given before Senate and congressional committees, and in documents produced by the General Accounting Office.

Extremist organizations, criminal groups and governments are acquiring expertise in the area of IO and could threaten various systems if they possessed the proper tools and techniques to exploit vulnerabilities, and the intent to do so. Testimony provided during committee hearings held within the United States revealed that an increasing number of countries have or are developing offensive IO

programs. Further, data indicates that an increasing number of extremist groups and intelligence services are becoming proficient in the development and / or use of IO tools and techniques. A number of these hostile actors may intend to use IO tools to achieve specific goals. Recent media reports indicate that protected military networks in the United States have been easily hacked using rudimentary tools. One American government-sponsored exercise (Eligible Receiver) demonstrated that software tools obtained from hacker sites on the Internet can not only degrade the operations of government departments but threaten the critical infrastructure.

In April 1998, hackers belonging to the "Masters of Downloading" (MOD), which an international membership, claimed they had broken into NASA and DoD classified computerized systems, having acquired the means to access these systems with impunity, and to control military satellite and other systems. With at least two Russian members, MOD was considered by computer experts to be more secretive, careful and sophisticated - and hence more dangerous - than Analyzer. MOD threatened to sell information about American systems to terrorist groups or foreign governments. MOD members allegedly communicate using an elaborate system of passwords and cover their tracks by routing messages through a variety of computer systems all over the world. Claims made by MOD have not been publicly corroborated to date.

In February 2000, national infrastructures suffered degradation from virus and distributed denial of service attacks (DDoS). The attacks, which centred on a number of companies, each with a significant presence on the Internet, were estimated to have caused damage in the order of billions of dollars. The subsequent infestation of computers around the world with the "I Love You" virus had even a more profound effect on systems and networks. This was due in part to the fact that the phrase "I Love You" in the subject line of an e-mail message was a simple psychological operations ploy that enticed many individuals to open the virus-laden e-mail attachment and infect their computer systems. The DDoS attacks of February 2000 acted as a proof of concept demonstrating that a number of computers previously compromised by hacker activity could be used in concert to focus attacks on a single target or a number of targets.

Political tensions have resulted in hacking duels between hacker groups and others in various countries. In 1999, there were hacking exchanges between China and Japan over the issue of the Nanking massacre, between China and Taiwan, and between India and Pakistan over Kashmir. In 2000, Armenians placed false information in the Azerbaijan daily Zerkalo, and the current tensions between Israel and Palestinians resulted in hacking activity by supporters of each side. The latter activity on the part of pro-Palestinian supporters expanded to include corporations and a pro-Israel organization in North America as targets.

Protection of the Canadian Critical Infrastructure

The Report of the Special Senate Committee on Security and Intelligence, published in 1999, addressed the issue of protecting Canada's critical infrastructure. The latter consists of both physical and cyber-based systems which are essential to the day-to-day operations of the economy and government. Historically, elements of this critical infrastructure were physically segregated. However, these elements gradually converged, became linked and more interdependent. Advances in computer and communications technologies resulted in a growing level of automation in the operation of critical systems. The report stated that the growth of, and our increased reliance on, the critical infrastructure, combined with its complexity, has made it a potential target for physical or cyber-based terrorism.

In its recommendations, the Committee suggested that the government take action to protect the critical infrastructure and to:

develop policies and resources to deal with any attacks;

create the capability to assess and reduce infrastructure vulnerabilities, and to prevent or respond to physical and cyber attacks;

create public-private sector partnerships to protect the critical infrastructure; and

ensure that the National Counterterrorism Plan regularly be reviewed and updated, especially relating to the impact created by new and emerging technologies that may be used by terrorists

The Canadian government responded to these recommendations by creating the Office of Critical Infrastructure Protection and Emergency Preparedness. The role of this agency is to work closely with the provinces and municipalities, private industry and other countries to protect Canada's electronic infrastructure against possible cyber-based attacks and natural disasters. In 2003, the agency was amalgamated into the Public Safety and Emergency Preparedness department.

In addition, each federal government department and agency has information technology (IT) policies and procedures. The Communications Security Establishment (CSE) advises the federal government on the security aspects of government automated information systems.

The Role of CSIS

The CSIS Information Operations program was initiated in 1997. As with all CSIS investigations, this program derives its authority from the CSIS Act. Under sections 2 (a) (b) and (c) of the Act, threats to the security of Canada are defined as: espionage or sabotage, foreign influence activities, or serious acts of violence against persons or property in support of achieving a political objective. The information operations threat may fall under any of these three sections.

The Service focuses its investigations on threats or incidents where the integrity, confidentiality, or availability of critical information infrastructure is affected. As a result, three conditions must appear in order to initiate a CSIS "information operations" investigation. That is, the incident:

a) must be a computer-based attack

b) must, within reason, appear to be orchestrated by a foreign government, terrorist group or politically motivated extremists;

c) must be done for the purpose of espionage, sabotage, foreign influence or politically motivated violence.

This definition excludes many of the computer intrusions occurring within Canada. For example, most hacking activity is being done by thrill-seeking amateurs with no political agenda. Moreover, a certain amount of hacking is conducted by criminals for monetary gain and by corporations seeking an unfair competitive advantage over another company. These types of computer intrusions fall outside the CSIS mandate but may be of interest to law enforcement. The Service confines its investigation to computer intrusions conducted with a "political motivation". That is, whether a hostile intelligence service is

hacking into Canadian computer systems, or an extremist group is targeting a government Web site - there must be a political aspect to the computer intrusion in order for CSIS to be involved.

Since the threat from cyber sabotage and cyber terrorism is part of a broader economic threat to key sectors of Canadian society, CSIS works closely with other government departments such as the Royal Canadian Mounted Police, the Department of National Defence and the Communications Security Establishment.

Furthermore, within the international milieu, CSIS liaises and exchanges information with allied agencies to remain abreast of the global threat and how it may affect Canada's national security. CSIS also participates with the federal government in broader G-8 efforts aimed at addressing the cyber threat.

Outlook

One of the greatest challenges in countering the threat in the realm of IO is that borders have become meaningless to anyone operating in a virtual environment. Even if great diligence was taken in the effort to remove vulnerabilities, it would be almost impossible to eliminate them entirely because attack tools, networks and network control systems are in a constant state of evolution.

As new technologies develop, so too will new attack tools and mechanisms. As a result, governments will have to set procedures in place to allow security initiatives to evolve to deal with new threats as they arise. For example, the risks involved with the movement of the private sector to an e-commerce environment, the initiatives within the private sector to provide services and system interconnection through wireless means, and the use of personal digital assistants all present challenges from a security perspective.

Hacking is becoming easier to a certain extent because some elements of both the private and public sectors around the world have been more interested in connecting to the Internet than in facilitating their operations securely via the Internet.

National Liaison Awareness Program

CSIS maintains a national Liaison Awareness Program. The program seeks to develop an ongoing dialogue with both public and private organizations concerning the threat posed to Canadian interests from cyber-based attacks. The purpose of the program is to enable CSIS to collect and analyse information that will assist it in its investigation of these threats which could have implications for Canada's national security. The Service then assesses the threat, and provides advice to government accordingly. This program is an important vehicle used by the Service to articulate its message to the Canadian public.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

Backgrounder: Collection of Security Intelligence Outside of Canada

June 2007

Why is it important to collect security intelligence outside of Canada?

In order to carry out its role of identifying and reporting on threats to Canada's security, the Canadian Security Intelligence Service (CSIS) must pursue all intelligence leads, whether national or international in origin. Given that many current threats to Canada's security originate outside of Canada's borders, CSIS is increasing its information collection capacity at the international level.

Does CSIS have a legal mandate to collect information abroad?

Section 12 of the CSIS Act directs the Service to collect, analyse and retain information and intelligence on activities that may, on reason-able grounds, be suspected of constituting a threat to the security of Canada. It places no geographic restrictions on intelligence gathering.

The Security Intelligence Review Committee, the external body that reviews CSIS, has stated that the Service has a clear mandate to conduct Section 12 investigations outside Canada.

CSIS has conducted operations abroad since its inception; with the evolving nature of the threat, these operations are increasingly com-plex and sophisticated.

What are the main international security threats to Canada?

Terrorism, particularly that which is inspired by the ideology of Al Qaeda, is the primary interna-tional threat to Canadian security. Counter-terrorism is consequently the Service's inves-tigative priority. Other investigative priorities include the proliferation of weapons of mass de-struction and the activities of hostile intelligence agencies in Canada, including economic espio-nage and interference in émigré and

expatriate communities. These complex and challenging threats require the Service to be increasingly proactive and sophisticated in its intelligence-gathering efforts outside of Canada.

How does CSIS gather intelligence abroad?

Overt collection

The CSIS Act allows the Service to enter into an arrangement with a foreign intelligence or law enforcement agency, after obtaining approval from the Minister of Public Safety and consulting with the Minister of Foreign Affairs. Currently, the Service has about 270 cooperative relation-ships with more than 145 countries, giving it access to global information and intelligence on potential terrorist threats.

The Service has Foreign Officers posted overseas, including at Canadian missions in London, Paris and Washington.

Covert Collection

When necessary, the Service may engage in covert operational activities outside of Canada. These activities are varied in nature, but all are conducted in accordance with the CSIS Act, CSIS policy and Ministerial Direction, and with appropriate approvals in place.

The combination of overt and covert information collection allows the Service to produce the kind of strategic intelligence and advice that govern-ment decision-makers need to deal with today's complex international security threats.

Contact

For comments/enquiries, please contact the Canadian Security Intelligence Service (CSIS)

c/o P.O. Box 9732, Postal Station T

Ottawa, Ontario, KIG 4G4.

Telephone 613-231-0100

or fax 613-231-0612.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

ARCHIVED: Backgrounder No. 13 - The Integrated Threat Assessment Centre (ITAC)

Backgrounder No. 13 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

April 2007

ARCHIVED: PDF version [192 KB]

Building an Integrated Security System

The Government of Canada, as part of its National Security Policy, is building a fully integrated security system, to enable Canada to respond more effectively to existing and emerging threats to its national security. The necessity for an integrated security system has become increasingly evident in recent years, most dramatically demonstrated by the events of September 11, 2001, and the numerous and widespread terrorist attacks since then. The requirement to encourage information-sharing and cooperation among organizations that collect and analyze intelligence vital to national security is paramount.

Meeting the challenge

An effective security system begins with a comprehensive threat assessment. While many individual departments and agencies produce threat assessments, their ability to share information and conduct effective analysis has been inconsistent in the past. To address this gap, the Government of Canada established the Integrated Threat Assessment Centre (ITAC), which has been operational since October 15th, 2004.

ITAC's Role

ITAC's primary objective is to produce comprehensive threat assessments, which are distributed within the intelligence community and to first-line responders, such as law enforcement, on a timely basis. Its assessments, based on intelligence and trend analysis, evaluate both the probability and potential consequences of threats. Such assessments allow the Government of Canada to coordinate activities in response to specific threats in order to prevent or mitigate risks to public safety.

Administration and Governance

With a budget of 30 million dollars over five years, ITAC is a functional component of the Canadian Security Intelligence Service (CSIS). It is housed within CSIS headquarters in Ottawa, and supported 24/7 by the CSIS Threat Management Centre.

ITAC works closely with the National Security Advisor (NSA) who, in consultation with the Director of CSIS, appoints ITAC's Director. Twice a year, the NSA chairs ITAC's Management Board meeting, attended by deputy ministers from participating organizations, to review ITAC's performance. An Assessment Management Committee, composed of assistant deputy ministers from participating organizations, provides advice to the Management Board on the focus, effectiveness and efficiency of ITAC activities. This committee and the NSA assist the ITAC Director in establishing threat assessment priorities. ITAC is required to submit an annual report to Cabinet.

A Cooperative Initiative

ITAC is a community-wide resource. It is staffed by representatives of the following organizations, who are usually seconded to the Centre for a period of two years:

Public Safety Canada

Canadian Security Intelligence Service

Canada Border Service Agency

Communications Security Establishment

Department of National Defence

Foreign Affairs and International Trade Canada

Privy Council Office

Transport Canada

Correctional Service Canada

Financial Transactions and Reports Analysis Centre of Canada

Royal Canadian Mounted Police

Ontario Provincial Police

Sûreté du Québec

These representatives bring the information and expertise of their respective organizations to ITAC. When required, ITAC can also draw upon the specialized knowledge of other federal government agencies, such as Agriculture and Agri-Food Canada, Health Canada, Environment Canada and Natural Resources Canada.

International Cooperation

Canadian security will increasingly depend on the country's ability to contribute to international security. Accordingly, the Government of Canada, through ITAC, is promoting a more integrated international intelligence community by cooperating with foreign integrated threat assessment centres, including the Joint Terrorism Analysis Centre, in Britain; the National Counterterrorism Center, in the United States; the National Threat Assessment Centre, in Australia; and the Combined Threat Assessment Group, in New Zealand.

Conclusion

ITAC is an essential component of the Government of Canada's efforts to build an integrated national security system. The centre facilitates increased information-sharing and integrated intelligence analysis. Its comprehensive threat assessments provide policy-makers and first responders with the information they need to make decisions and take actions that contribute to the safety and security of Canadians.

Contact

For comments or enquiries, please contact the Canadian Security Intelligence Service (CSIS):

CSIS

P.O. Box 9732

Postal Station T

Ottawa, Ontario

K1G 4G4

Telephone 613-231-0100 or

Fax 613-231-0612

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

ARCHIVED: Backgrounder No. 15 - Screening of Refugee Claimants

Backgrounder No. 15 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

February 2004

Introduction

Beginning in November 2001, the Government of Canada adopted a new policy which requires that all refugee claimants to Canada be subject to Refugee Claimant Screening. This process involves checking refugee claimants against CSIS and RCMP records at the beginning of their determination process and in advance of Immigration and Refugee Board (IRB) hearings. The purpose of the program is to identify and filter potential security and criminal cases as early as possible in the refugee protection determination process. The Refugee Claimant Screening program is conducted by the Security Screening Branch of the Canadian Security Intelligence Service (CSIS) for the purpose of providing security-related advice to the Minister of Citizenship and Immigration (CIC).

Who are Refugee Protection Claimants?

Canada has signed the 1951 Convention Relating to the Status of Refugees and its 1967 Protocol. Refugee protection is conferred on persons when the IRB determines that they are Convention refugees or persons in need of protection.

A Convention refugee is a person outside of their country of nationality or habitual residence who is unable or unwilling to return to that country because of a well-founded fear of persecution for reasons of race, religion, political opinion, nationality or membership in a particular social group.

A person in need of protection is a person in Canada whose removal to their country of nationality or former habitual residence would subject them to the possibility of torture, risk to life, or risk of cruel and unusual treatment or punishment.

Wars, famines, natural disasters, or state policies, such as ethnic cleansing, are common reasons for people to flee their homelands. Between 20,000 and 30,000 persons request refugee status annually in Canada and now all will require security checks.

Reasons for Adopting Refugee Claimant Screening

Refugee Claimant Screening is a relatively recent government initiative through CIC, to ensure that all refugee claimants arriving in Canada are subject to a screening process similar to that used for applicants for permanent residence. The Security Screening Branch of CSIS has, however, been conducting for a number of years security screening of those Convention refugees and all other immigrants who apply for permanent residence status from both within and outside of Canada. It has also provided advice to the Minister of Citizenship and Immigration related directly to the security inadmissibility criteria contained in the Immigration and Refugee Protection Act (IRPA). The branch also provides CIC with security assessments on applicants for Canadian citizenship.

The fairness of Canada's refugee determination system is recognized around the world, but was deemed vulnerable to abuse. The Government of Canada planned to improve the refugee determination system through a balanced series of measures that would preserve Canada's tradition of offering protection to genuine refugees, while increasing integrity and effectiveness. By adopting a Refugee Claimant Screening program, the government has taken action to ensure that our immigration and refugee determination systems are not open to abuse by criminals or terrorists.

Prior to November 2001, refugees would only be screened once they applied for permanent resident status in Canada. To apply for permanent residence, a person must have been determined to be a Convention refugee by the IRB. However, many refugee applicants were never screened as they never applied for permanent resident status. The fact that the government could not determine for certain the whereabouts of unscreened refugee claimants, combined with the fact that it can take a year or more between application for refugee status and a hearing, meant that thousands of unscreened refugee claimants could be living in Canada at any time.

The issue of unaccounted refugee claimants was a source of concern for a number of reasons, some of which were security-related. One such reason was the potential for terrorists to slip into Canada as part of the refugee stream. Another was the possibility that certain people could attempt to use refugee status to bring foreign-rooted issues to Canada, undermining domestic security within this country.

This situation led the Government of Canada to conclude that a security gap existed in the refugee immigration stream. The Refugee Claimant Screening program was introduced in order to close this security gap. This program seeks to identify and filter potential security and criminal cases from the refugee claimant stream as early as possible in the determination process, thereby strengthening the integrity of the refugee determination process and enhancing public safety.

How Is Screening for Refugee Claimants Conducted?

Refugee claimants may make a claim for refugee protection at any CIC Port of Entry (POE) office (airport or land border crossing) or inland CIC office across the country. In the case of applicants where no initial security concerns are noted by the CIC officer, the refugee claimants' background information is forwarded by CIC to the CSIS Security Screening Branch to conduct its screening checks.

A second distinct, yet complementary, program assists in identifying refugee claimants who are inadmissible for security reasons as early as possible in the refugee determination process. This program is known as the Port of Entry Interdiction Program (POEIP). Should a front- line CIC officer posted at a port of entry have security concerns pertaining to an individual's inadmissibility to Canada, the officer may request the assistance of a CSIS officer to conduct a joint interview of the individual and to provide security-related advice. By screening those with security concerns at the port of entry, the POEIP seeks to prevent persons who are inadmissible under IRPA from entering or gaining status in Canada. Since the

events of September 11, 2001, CSIS is present at selected border crossings and international airports to assist Immigration and Customs officers.

As with all of its immigration screening programs, the Service advises if any security concerns relating to a particular application surface in the course of its checks and provides CIC with relevant security advice if such concerns come to light. In all immigration and citizenship applications, the Minister of Citizenship and Immigration has the ultimate responsibility of determination for the application.

Part of the Government's Overall Commitment to National Security

Screening of Refugee Claimants is part of the Government of Canada's overall commitment to protect Canada's national security interests. With between 20,000 and 30,000 refugee claims annually, Refugee Claimant Screening serves as a first line of defence against those who would act against Canada's citizens or interests by using its refugee policies to gain access to the country. CSIS, through its Security Screening Branch, assists the Minister of Citizenship and Immigration Canada to ensure that those who are inadmissible to Canada for reasons of security are identified and prevented, as rapidly as possible, from taking up residence in Canada.

ARCHIVED: Backgrounder No. 16 - Operations Abroad

Backgrounder No. 16 has been archived.

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

May 2004

Introduction

This Backgrounder, one of a series, will attempt to put into context the issue of Canada's security intelligence operations outside of Canada - in part because there continue to be questions, and perhaps some confusion, about the issue (often resulting from definitional problems) and in part because the nature and scope of CSIS operations abroad have changed over the years.1

Section 12 of the CSIS Act sets out the primary mandate of the Service: Collecting information and intelligence related to "threats to the security of Canada", a term defined in section 2 of the CSIS Act.2

Historical Background

Canada's first security intelligence organization was established by Sir John A. Macdonald before Confederation. It operated in a small area along the borders of Upper Canada, crossing over that border

to secretly collect information on the Fenians and the implications of the American Civil War for Canada's security.

At the turn of the century, rumours of American plots to annex the Yukon were investigated through the surveillance of suspected plotters in the United States and Canada, and by infiltrating some American miners' organizations.

The First World War saw further activities in the United States directed against agents suspected of espionage and subversion. Before the United States' entry into World War I, the Commissioner of the Royal North West Mounted Police directed, from the force's headquarters in Regina, investigations on persons of German and Austrian extraction suspected of launching espionage or sabotage activities against Canada from the western United States.

When the RCMP became responsible for collecting security intelligence in 1920, it adopted the policy of restricting its covert operations to within Canada. This practice changed with the creation of first Special Branch and later the RCMP Security Service. In its 1981 report, the McDonald Commission described the (then) current practice as follows:

Covert Security Service operations outside Canada today are conducted on an ad hoc basis. These cases involving foreign travel always arise from an internal security investigation begun in Canada. Generally, the rationale for such operations is that the information sought relates directly to the internal security of Canada and is not the kind of information that can be or should be obtained through liaison with friendly security and intelligence agencies.

The McDonald Commission

In considering what might constitute an appropriate framework for meeting Canada's security needs, the McDonald Commission considered the proper scope of security intelligence activities outside Canada. In doing so, the Commission discussed the distinction between "offensive" and "defensive" intelligence agencies, finding those terms somewhat confusing and unhelpful since the distinctions could refer to any one of the three following and different ways of categorizing intelligence organizations:

(a) on the basis of the kind of intelligence collected

Intelligence is often divided into categories such as "security intelligence" (threat-related) or "foreign intelligence" (non threat-related information about foreign individuals or states), the former sometimes within the purview of defensive services and the latter part of the mandate of offensive services.

(b) on the basis of the activities of a service

Services which engage in "covert" or "executive" actions such as assassinations or attempting to promote regime change in foreign countries are sometimes described as offensive services.

(c) on the basis of the geographic location of an agency's activities

Services which operate within their own country's borders are sometimes described as defensive services and those which operate outside sometimes as offensive services.

The Commission noted that the mandate it recommended for the new service could be considered to be "defensive" both in the sense that the intelligence to be collected must pertain to threats to the security of Canada, and in the sense that the service's mandate be confined to collecting and analysing information and producing intelligence. However, in discussing the geographic location of a security intelligence agency's activities, McDonald said:

If security intelligence investigations which begin in Canada must cease at the Canadian border, information and sources of information important to Canadian security will be lost. .... If to operate abroad is "offensive", then Canada's security intelligence agency should be offensive in this sense ....

The CSIS Act

When adopted in 1984, the CSIS Act reflected the McDonald Commission's recommendations with regard to the collection of security intelligence abroad.

As noted earlier, section 12 of the CSIS Act defines the Service's primary operational mandate and was consciously drafted to contain no restriction at all about where the Service may collect such information. Further, nothing prohibits the Service from retaining intelligence related to foreign states or persons if the information is acquired in relation to the investigation of the threats under section 12.

As the (then) Solicitor-General Bob Kaplan said during debate on the Bill:

there is no statutory requirement that the entire activities of the Security Intelligence Service be performed in Canada. I think that would be unduly inhibiting.

Though the specific challenges that Canadian national security might face in the future were unpredictable, those responsible for drafting the legislation foresaw the need for a legal framework that would enable the new service to adapt to changes in the global security environment.

While the CSIS Act places no geographic limits on the collection of intelligence about threats to the security of Canada nor on the techniques, covert or otherwise, used in such collection, CSIS is restricted in its ability to collect non threat-related foreign intelligence 3 In relation to the defence of Canada or the conduct of the international affairs of Canada. While security intelligence collection remains the priority for the Service, the collection in Canada of such non threat-related foreign intelligence has been a growing part of the Service's operations.

The Changing Threat

In the early days of CSIS, the majority of the operational resources of the Service were dedicated to threats from espionage, clandestine foreign interference and subversion (the latter ending with the closure of the Service's Counter Subversion branch in 1988). While operations were conducted abroad in response to unique and specific circumstances (for instance, in relation to an East Bloc defector or an existing human source who had access to unique information abroad), this type of activity was the exception rather than the norm.

Over time, however, CSIS has shifted its operational priorities to meet requirements related to public safety, most notably exemplified in the growing threats of international terrorism and the proliferation of weapons of mass destruction. By 1989/1990, the Service's operational priorities, on which Cabinet is consulted, specified public safety as the number one requirement, a ranking which remains current.4

Given that virtually all current threats to the security of Canada either have their origins abroad or are manifested across international borders, CSIS has had to increasingly look outside Canada's borders, both to understand the threat and to build strong cooperative relationships with intelligence services around the world. As a result, the number of liaison arrangements with foreign security and intelligence organizations has grown - from around 50 in the late 1980s to nearly 250 today.

In addition to overt liaison activity, foreign covert operational activities have also been expanded and changed. In the mid-90s this often meant cooperating with a sister service from another country, establishing joint operations to obtain information of mutual security concern. Such operations remain an important part of the Service's repertoire. Since the late 90s, however, always subject to resource considerations and a careful risk assessment, the Service has increasingly engaged in covert foreign operations. This change was due, in part, to the changing nature of the threat; it was also a logical development of the Service's growing experience in these operations and, lastly, because of our country's often unique access to individuals and sources able to provide information about threats to the security of Canada. Our centralized information holdings, which include all intelligence (whether collected domestically, outside of Canada or received from liaison partners) enable the Service to fully analyse this information, all subject to full access and review by our review agencies.

Current Practice

The accelerating international dimensions of the terrorist threat have seen foreign collection techniques employed more frequently. As expertise has grown, CSIS's foreign operations have expanded to include, amongst others, such techniques as: tasking human sources to travel abroad, recruiting foreign sources, meeting those sources in third countries.

As the (former) Solicitor General noted in Parliament in 2001:

Mr. Speaker, what I am telling my honourable colleague, and I have said this many times in the House, is that CSIS has the authority to investigate, inside of this country and outside of this country, any activity that threatens Canada. That is the mandate of CSIS.

As noted earlier, subject always to resource considerations and a careful assessment of the risk, CSIS will continue to consider the use of covert intelligence operations outside of Canada if it will assist in investigating and better informing the government about the threats that we face to our national security.

1 For more information on the history and mandate of CSIS, refer to other Backgrounders available on the CSIS Web site. Titles include: The CSIS Act; The CSIS Mandate; Accountability and Review; and CSIS and the Intelligence Cycle.

2 For the exact wording of both section 12 and the definition of "threats to the security of Canada" in section 2, refer to the CSIS Act available on the CSIS Web site.

3 "Foreign intelligence" in the context of section 16 of the CSIS Act means "information or intelligence relating to the capabilities, intentions or activities of (a) any foreign state or group of foreign states; or (b) any person other than [a Canadian]. Under section 16, CSIS may assist in the collection of such information but only within Canada and only on the personal request of the Minister of National Defence or the Minister of Foreign Affairs and International Trade and with the consent of the Solicitor General.

4 For further information on how the nature of terrorism has changed and what the response of Canada and CSIS has been, please refer to various CSIS publications such as: International Terrorism: the Threat to Canada or Operational Programs: Counter-Terrorism available on the CSIS Web site.

ARCHIVED: Backgrounder No. 17 - Control, Accountability and Review

May 2005

Archived Content

Information identified as archived on the Web is for reference, research or recordkeeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards. As per the Communications Policy of the Government of Canada, you can request alternate formats on the "Contact Us" page.

I. Breaking New Ground: The CSIS Act & Review

In 1969, the Royal Commission on Security (the Mackenzie Commission) published a report. Its principal recommendation was to establish a civilian agency, separate from the Royal Canadian Mounted Police, to assume the security intelligence function in Canada. The Commission, in considering effective "security methods and procedures", neither explored nor recommended mechanisms for independent, external-to-government review.

After four years of work, the McDonald Commission1 reported in 1981 and advanced, like Mackenzie, the central proposal for a civilian security intelligence service for Canada. McDonald did not content himself with narrow prescriptions for a legislated mandate and internal, or internal-to-government, mechanisms to ensure the new agency's proper functioning. The Commission Report made extensive recommendations for what it termed "External Controls". These included:

the Federal Court, to deal with issues of disclosure and intrusive investigative techniques;

a Security Appeals Tribunal, to hear appeals about denial of security clearances;

an Advisory Council on Security and Intelligence, to be independent and arm's-length. Among other functions, it would conduct a continuous review of policy and practices with retroactive force to ensure legality and propriety. It would have access to all information and files, investigate complaints in certain circumstances, and report to the Minister and a Committee of Parliament;

a Joint Parliamentary Committee of the House and Senate, to monitor the "effectiveness and propriety" of the new Service.2

In August, 1981, the Government responded to the McDonald Commission Report by announcing that the Security Service would be separated from the RCMP and established as a civilian security intelligence agency. A transitional group was set up to study the McDonald recommendations in detail and to develop specific plans for creating the new agency, giving paramount consideration to five basic principles. The last of these stipulated that the new agency must "be open to a satisfactory external review, ensuring that the agency does not abuse its powers and that it is not misused by government".3

There followed nearly two years of intensive work by officials. The Cabinet Committee on Security and Intelligence, chaired by the Prime Minister, met several times to monitor progress and give guidance. The legislative phase was long, difficult and marked by:

intense scrutiny and debate, both public and parliamentary;

the original Bill (C-157) stalling in the House on First Reading and, as rarely seen, its subject matter referred to a Special Committee of the Senate;

extensive hearings by the Senate Committee and a public report calling for nearly four dozen amendments to Bill C-157;

subsequent Cabinet consideration and the tabling (in January 1984) of revised legislation, Bill C-9;

a further three months of hearings and study by the House Standing Committee on Justice and Legal Affairs.

Emerging from this process, Bill C-9 drew heavily on McDonald's Report and recommendations, accepting and validating the Commission's arguments in support of such proposals, leavened by the findings of the Special Senate Committee. And the resultant Canadian Security Intelligence Service (CSIS) Act, as McDonald had intended it should, accomplished far more than a mere charter for a security agency.

The CSIS Act established, in law, a comprehensive regime for the security intelligence function in Canada: a civilian agency with no executive terms of reference; with clearly (and where appropriate, precisely) defined mandate and powers; subject to a rigorous, inter-related system of political and judicial controls; and, importantly, subject to independent, arm's-length review. The centrepiece of that system for accountability, control and review was and is the unique combination of the Security Intelligence Review Committee (SIRC) and the Inspector General (IG)-the former reporting, through the Minister, to Parliament; the latter, in a more specialized but complementary way, acting as the "Minister's 'eyes and ears' on the Service".4

The review provisions of the CSIS Act were, in 1984, unprecedented in the world of intelligence and security intelligence agencies. Today, they remain unsurpassed by any other system of review in terms of scope, function and access to the records and personnel of the agency (CSIS) under review. Why unsurpassed? A simple, encompassing statement from SIRC's first Annual Report provides an answer:

"...the Committee will need to know, in considerable detail, virtually everything that is being done by CSIS".5

In combination with the Inspector General, SIRC represented a sea change in accountability for a security intelligence function whose activities were traditionally clothed in secrecy. In addition, the activities of the Service are, like those of other government departments and agencies, subject to the scrutiny of Officers of Parliament, namely the Auditor General, the Access to Information and Privacy Commissioners and the Commissioner of Official Languages.

II. Review - A Brief Retrospective

More than twenty years of experience with review allows the Service to offer the following observations. Any candid assessment must accept the fact that the CSIS-SIRC and CSIS-IG relationships involved a long, sometimes adversarial period of introduction, mutual adjustment, accommodation and consolidation. It can be argued that the relationships-particularly between CSIS and SIRC-took almost a decade to fully mature and work well. Indeed, that coincides with the experience in the United States, where the same time period applied to acceptance and full functioning of their process, which can be best described as oversight, as opposed to review of activities.

With experience, the Service not only learned to accept the need for, and reality of, review as part of the business of security intelligence, but fully internalized that concept. A dual expectation emerged that SIRC would:

report on instances of perceived unlawfulness, impropriety or over-zealousness; and, as well

report on incidents in which the Service was mistakenly or unfairly accused and, absent SIRC, had no effective or objective means of public defence.

For its part, SIRC (and importantly, its permanent research staff) gradually became more attuned to, and conversant with, the complex world of security intelligence, and the challenges that complexity presented to the Service. Without compromising their duty for rigour and scepticism, the Committee and its staff in time moderated an early posture of aggressive mistrust that complicated their relationship with the Service and its employees.

Over that twenty-year period, some early myths were exploded, and some fears laid to rest, regarding the potential adverse effect of the CSIS Act provisions for review. The most important of these was a feared "chilling effect" on Service operational aggressiveness and initiative-the prospect of review encouraging a risk-averse and ineffective Service. Though such negative effect is almost impossible to measure, the number and success of Service investigations in that two-decade span suggest that this "effect" has not been significant-if it existed at all.

Similarly, concerns that comprehensive SIRC/IG access to Service files would cause nervous international partners and liaisons to restrict intelligence exchanges have not, in the long run, come to pass. Related worries about SIRC/IG ability to afford proper security to Service information and protect its human sources and sensitive collection methodologies have not been justified-"leakage" of classified information has not been a factor.

Finally, early and continuing concerns had been expressed about the resource-intensive consequences of review: the spectre of a Service so tied up in responding to review-generated demands that it would have little time for "real work".

While the Service does not quantify the "dollar costs" of review, the resource implications for supporting and responding to requests from the SIRC and IG are not inconsequential. Some general information may give an appreciation of the extent of CSIS' daily involvement in this responsibility.

Under the Assistant Director, Secretariat (ADS), reporting to the Director of the Service, the External Review and Liaison (ER&L) section currently has 10 officers responsible for liaison with a current total of 24 staff at SIRC and the IG. While ER&L is responsible for managing all reviews undertaken by both organizations and identifying and retrieving information for review, the formal responses to a large number of written enquiries and verbal briefings on various investigations are channelled through more than a dozen operational and technical branch coordinators within the Service's headquarters and in the six regional offices. About sixty-five percent of the branch coordinators' time is spent on responding to requests related to SIRC and IG studies.

The CSIS Act also authorizes SIRC to hear complaints on any action of the Service (s.41) and on the denial of a security clearance (s.42). If the Committee determines that the complaint should proceed to a

formal hearing, the Service is required to present testimony through CSIS witnesses and legal counsel-a resource-intensive undertaking.

Both review bodies travel to CSIS regional offices regularly to conduct interviews of employees and to obtain information on investigative activities in the regional environment. SIRC and the IG undertake an annual audit of a regional office, which typically sees three to six reviewers conducting interviews in a region over a three-to five-day period-a concentrated exercise which occupies a large number of regional resources. Additionally, a three-day audit of one of the Service's foreign liaison posts is done yearly by SIRC.

Liaison with SIRC and the IG takes place at all levels, and includes regular meetings with the senior management and Executive members of the Service. Over the course of a year, the Committee meets with the Director at least twice, in addition to meeting with two or three regional management teams. Those meetings are formal in nature, with the Committee supplying a series of questions to the region in advance, and spending a half-day with the regional management team. The Inspector General meets annually with regional Directors General and their management teams, and with the majority of Directors General in Headquarters.

III. SIRC and the IG - Their Role and Practical Effect

The following section provides some insight into the day-to-day activities of the review bodies and the measures they take to fulfill their function.

CSIS Act s.38 sets out the fundamental function of the SIRC: "to review generally the performance by the Service of its duties and functions" and, in s.40, the purpose of such review: "ensuring that the activities of the Service are carried out in accordance with [the] Act, the regulations and directions issued by the Minister, ... and that the activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers, ..."6

Twenty years of reviewing CSIS work have focussed SIRC methodologies and work plans. In concert, these are designed so that over time there are no Service corners into which the light of review has not shone. In choosing activities on which yearly, detailed reviews will concentrate, SIRC "takes into consideration such matters as the scope and importance of CSIS investigations, the potential for particular activities to intrude on individual rights and liberties, priorities and concerns for Parliament

and the Canadian people, the CSIS Director's report on operational activities, and the importance of producing regular assessments of each of the Service's branches. Each report is the result of a detailed review of CSIS documents, interviews with Service staff and senior managers, and an assessment of the Service's actions in relation to applicable laws, policies and Ministerial Direction".7

That approach is augmented by additional factors:

world events and their impact on threats to the security of Canada;

trends or concerns identified in previous Committee reports;

commitments by the Committee to re-examine specific issues or investigations;

issues identified in the course of the Committee's complaints function;

new policy directions or initiatives announced by the Government of Canada; and

the Committee's statutory duties under the CSIS Act. 8

SIRC reviews in the last two reporting years (2002-03 and 2003-04) are instructive in demonstrating the encompassing reach of the Committee. During that two-year span they examined, in detail:

CSIS Front-end Screening Program for Refugee Claimants;

Section 12 (CSIS Act) Operational Activity Outside Canada;

a Counter Intelligence (CI) Investigation;

a Counter Proliferation (CP) Investigation;

Liaison with Foreign Agencies - A Review of a Security Liaison Post;

an Internal Security Breach in a Regional Office;

An (Annual) Review of Foreign Arrangements;

the Ressam Case;

Sunni Islamic Extremism - A Review of a CSIS Regional Investigation;

Domestic Threats in Conjunction with Lawful Advocacy, Protest and Dissent;

Collection of (s.16 CSIS Act) Foreign Intelligence.9

The SIRC examination of the CI & CP investigations bears comment. In its review of specific operational cases, the Committee employs a standard methodology refined over two decades. In such cases, it assesses Service compliance with the CSIS Act, Ministerial Direction and CSIS Operational Policy by concentrating on key operational activities:

targeting decisions and investigations;

implementation of warrant powers and special operations;

management of human sources and sensitive operations;

cooperation and exchanges of information with domestic partners;

cooperation and exchanges of information with foreign partners; and,

advice to government.10

All of that to the end of determining whether:

the Service had reasonable grounds to suspect a threat to the security of Canada [i.e. an "investigative threshold" test11]

the level of intrusiveness of the investigation was proportionate to the seriousness and imminence of the threat [i.e. a "proportionality" test12] and

the Service collected only that information strictly necessary to fulfill its mandate to advise the Government of a threat [i.e. the test of "necessity"13]14

In addition to the conduct of such in-depth reviews, SIRC monitors Service "Plans and Priorities", particularly in respect of the major Operational and Analytical Branches (Counter Terrorism; Counter Proliferation; Counter Intelligence; Security Screening [including Citizenship & Immigration Screening]; and, Research, Analysis & Production). This is accomplished through extensive oral and written briefings, and also allows the Committee to fulfill its s.38(a)(vii) CSIS Act requirement to compile and analyze statistics on Service operational activities. All of this is in addition to SIRC's responsibility to hear public complaints against CSIS "with respect to any act or thing done by the Service".15

It is also worth noting that SIRC's work plan is, each year, parallelled by that of the Inspector General who-quite separately-pursues her own examination of the Service's activities to determine their compliance with law and policy. In the Certificate of November 2003, the Inspector General's annual program of review activities was summarized as including:

reviews of samples of warrants and targets, as well as of human source management;

detailed examinations of investigations of the threat posed [- -];

a review of section 16 intelligence collection;

a special study of the Service's domestic liaison arrangements;

comprehensive briefings on the front-end screening program of refugee claimants [- -]

As the Review Committee observed in its 1989-90 Annual Report, "not many public institutions get the kind of close attention that we give CSIS, or the publicity that goes with it. But independent review is the trade-off for the powers that an intelligence agency has- and needs-to intrude on individual privacy for the sake of national security." In sum, the review provisions of the CSIS Act-embodied in the SIRC and the IG-have proven, over time, to have worked as Parliament intended: an uncompromising, non-

shaded window on the Service, whose critical (or affirmative) voice is heard by responsible Ministers, Parliament and the public at large.

The Review Committee can-and has-articulated examples of how its scrutiny and subsequent reporting have influenced positive changes in Canada's security intelligence posture and landscape, benefiting Canadians and their security intelligence service. Those need not be repeated here.

The SIRC/CSIS relationship has best been characterized as one of healthy tension. The Committee has, within the context of its legislated responsibility, the duty to maintain its distance, scepticism and capacity for fully independent, critical audit: in short, its "watchdog's" teeth and credibility.

IV. Other Controls

The controls exercised by SIRC and the IG do not comprise the sole check on Service activity. Extensive internal controls and accountability ensure the work of the Service is not just effective, but also in conformity with the law, Ministerial Direction and propriety, and is proportionate to the nature and seriousness of security threats.

The principal animating factor of CSIS internal controls is the Service's highly centralized nature-a centralization that extends to, and impacts upon, all aspects of operational decision-making. Most importantly, central operational control is manifested in two committees chaired by the Director, CSIS:

the Target Approval and Review Committee (TARC). It includes the most senior Service operations managers, Department of Justice counsel and a designate of the Deputy Minister of Public Safety and Emergency Preparedness. It decides which groups or individuals will be subject to Service investigation and the level of intrusiveness appropriate to each. Thus, the origins, scope and intrusiveness of all investigations are initiated and controlled at the most senior level.

the Warrant Review Committee (WRC). Having the same membership as TARC, with the notable addition of an Independent Counsel, it reviews and approves all s.21 CSIS Act warrant applications to the Federal Court. Thus, the most intrusive investigative powers of the Service are subject to the most senior level of examination and approval before they are requested from the Federal Court. In considering these warrant applications, the Federal Court provides the essential element of judicial

control on CSIS investigative powers-powers having the greatest potential to affect individual rights and freedoms.

Another unique provision of the CSIS Act, set out in section 20 of the legislation, is designed to ensure the reporting and investigation of all cases where CSIS employees may have failed to comply with legislation or policy or committed an unlawful act in the performance of their duties. The purpose of this section is to require the reporting of alleged unlawful activities that may otherwise have remained undetected by provincial law enforcement agencies.

Finally, CSIS internal controls operate within a broader framework of direction and accountability, most importantly including the Minister, and Parliament. A more detailed summary of the CSIS accountability and review framework and the security intelligence cycle it regulates, can be found on the CSIS Web site.16

V. Conclusion

In considering the dynamic between external review and internal controls, a note of balance was struck by Maurice Archdeacon in his 2003 Inspector General's Certificate. Mr. Archdeacon was Executive Director of SIRC from its inception until 1 September, 1999, when he was appointed Inspector General. He retired in November, 2003:

"In my opinion, in the nearly twenty years during which I have had some knowledge of these matters, the Service has evolved from being a rather disorganized organization with significant weaknesses, to a highly professional and effective arm of government.

Most of this substantial improvement in performance can be credited to the senior managers and staff of the Service. Without their determined and well-directed efforts, no amount of outside pressure could have achieved the same result.

Nevertheless, the existence and, from time to time, the observations of the two outside review agencies have certainly contributed to the maturing process. I hope, as I retire from active participation in this challenging environment, that no-one makes the mistake, so often made in the past, of believing that current safeguards are no longer really necessary. The low costs of the review bodies and the very special care taken in the selection of the Director of the Service are a very small price indeed to pay for a professional, effective, and virtually trouble-free security service in these dangerous times."[17]

Appendices:

1 The Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police.

2 McDonald Commission Report, 2nd Report, Vol. 2

3 Canadian Security Intelligence Service - Explanatory Notes, Solicitor General Canada, May 1983, p.2.

4 Report of the Special Committee of the Senate on the Canadian Security Intelligence Service [Pitfield Committee], p. 29.

5 Security Intelligence Review Committee Annual Report 1984-85, p. 5

6 s.38 and s.40, CSIS Act

7 SIRC Report 2003-2004, p. 3

8 SIRC Report 2003-2004, p. 4

9 SIRC Reports 2002-03 and 2003-04

10 SIRC Report 2003-04, p. 16

11 Emphasis added

12 Emphasis added

13 Emphasis added

14 SIRC Report 2003-04, p. 16

15 s.41, CSIS Act

16 "Accountability and Review", Canadian Security Intelligence Service, Backgrounder Series, No.2, November 2004.

"CSIS and the Security Intelligence Cycle", Canadian Security Intelligence Service, Backgrounder Series, No.3, February 2004.

17 Certificate of the Inspector General of the Canadian Security Intelligence Service, 2003, op.cit.

Contact

For comments/enquiries, please contact the Canadian Security Intelligence Service (CSIS)

c/o P.O. Box 9732, Postal Station T,

Ottawa, Ontario, KIG 4G4.

Telephone 613-231-0100

or fax 613-231-0612.

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

Backgrounder: Collection of Security Intelligence Outside of Canada

June 2007

Why is it important to collect security intelligence outside of Canada?

In order to carry out its role of identifying and reporting on threats to Canada's security, the Canadian Security Intelligence Service (CSIS) must pursue all intelligence leads, whether national or international in origin. Given that many current threats to Canada's security originate outside of Canada's borders, CSIS is increasing its information collection capacity at the international level.

Does CSIS have a legal mandate to collect information abroad?

Section 12 of the CSIS Act directs the Service to collect, analyse and retain information and intelligence on activities that may, on reason-able grounds, be suspected of constituting a threat to the security of Canada. It places no geographic restrictions on intelligence gathering.

The Security Intelligence Review Committee, the external body that reviews CSIS, has stated that the Service has a clear mandate to conduct Section 12 investigations outside Canada.

CSIS has conducted operations abroad since its inception; with the evolving nature of the threat, these operations are increasingly com-plex and sophisticated.

What are the main international security threats to Canada?

Terrorism, particularly that which is inspired by the ideology of Al Qaeda, is the primary interna-tional threat to Canadian security. Counter-terrorism is consequently the Service's inves-tigative priority. Other investigative priorities include the proliferation of weapons of mass de-struction and the activities of hostile intelligence agencies in Canada, including economic espio-nage and interference in émigré and

expatriate communities. These complex and challenging threats require the Service to be increasingly proactive and sophisticated in its intelligence-gathering efforts outside of Canada.

How does CSIS gather intelligence abroad?

Overt collection

The CSIS Act allows the Service to enter into an arrangement with a foreign intelligence or law enforcement agency, after obtaining approval from the Minister of Public Safety and consulting with the Minister of Foreign Affairs. Currently, the Service has about 270 cooperative relation-ships with more than 145 countries, giving it access to global information and intelligence on potential terrorist threats.

The Service has Foreign Officers posted overseas, including at Canadian missions in London, Paris and Washington.

Covert Collection

When necessary, the Service may engage in covert operational activities outside of Canada. These activities are varied in nature, but all are conducted in accordance with the CSIS Act, CSIS policy and Ministerial Direction, and with appropriate approvals in place.

The combination of overt and covert information collection allows the Service to produce the kind of strategic intelligence and advice that govern-ment decision-makers need to deal with today's complex international security threats.

Contact

For comments/enquiries, please contact the Canadian Security Intelligence Service (CSIS)

c/o P.O. Box 9732, Postal Station T

Ottawa, Ontario, KIG 4G4.

Telephone 613-231-0100

or fax 613-231-0612.